# 目次

## 第 5 章 認証デバイスの取り扱い



## 第 6 章 こんなときには



## 第 7 章 付録

# はじめに

このたびは弊社製品をご購入いただき、誠にありがとうございます。
このマニュアルは、指紋センサーやセキュリティチップなどの認証デバイスの基本的な取り扱い、認証デバイスをお使いになるためのソフトウェア「SMARTACCESS」のインストール、および設定と使い方について説明しています。
お使いになる前に、このマニュアル、およびコンピュータ本体のマニュアルをよくお読みになり、正しくお使いいただきますようお願いいたします。

2007 年 10 月

## ■セキュリティ機能について

・セキュリティ機能は完全な認証照合、データやハードウェアの保護を保証するものではありません。弊社は、お客様がセキュリティ機能を使用されたこと、または使用できなかったことによって生じるいかなる損害に関しても、一切の責任を負いかねますのであらかじめご了承ください。
・認証デバイスは、コンピュータ用機器として設計されております。人命に関わる用途、または高度な信頼性、安全性を要する用途での使用は考慮されておりません。このような用途で使用される設備、機器、システム等への組み込みは避けてください。
・認証デバイスは日本国内仕様であり、添付のアプリケーション、ドライバなどは Windows の日本語版のみ対応しております。

# SMARTACCESS のマニュアルについて

「SMARTACCESS」には、次のマニュアルを用意しております。目的に合わせてお読みください。

## ■SMARTACCESS ファーストステップガイド（認証デバイスをお使いになる方へ）

このマニュアルです。
認証デバイスのドライバインストール手順、設定手順と取り扱い方、および SMARTACCESS のインストール、アンインストールと初期設定手順を説明しています。

## ■SMARTACCESS/Basic リファレンスガイド

このマニュアル内では、『リファレンスガイド』と表記します。
SMARTACCESS の機能を「機能編」と「ツール編」に分けて説明しています。
・機能編
　代表的な機能と使い方を、目的別に説明しています。
・ツール編
　機能全般を、メニューに沿って説明しています。

## ■スマートカード 証明書ガイド

Windows Server 2003 の証明書サービスを利用してスマートカードに証明書を登録し、Windows ログオンなどを行う方法について説明しています。

『リファレンスガイド』、『スマートカード証明書ガイド』は、コンピュータ本体に添付の「ドライバーズディスク」に格納されています。

# このマニュアルの表記

## ■本文中の記号

本文中に記載されている記号には、次のような意味があります。

| 記号 | 意味 |
|---|---|
| 重要 | お使いになる際の注意点や、してはいけないことを記述しています。必ずお読みください。 |
| POINT | 操作に関連することを記述しています。必要に応じてお読みください。 |
| → | 参照ページや参照マニュアルを示しています。 |

## ■キーの表記と操作方法

本文中のキーの表記は、キーボードに書かれているすべての文字を記述するのではなく、説明に必要な文字を次のように記述しています。

例：【Ctrl】キー、【Enter】キー、【→】キーなど

また、複数のキーを同時に押す場合には、次のように「＋」でつないで表記しています。

例：【Ctrl】＋【F3】キー、【Shift】＋【↑】キーなど

## ■コマンド入力（キー入力）

本文中では、コマンド入力を次のように表記しています。

```
diskcopy a: a:
         ↑  ↑
```

・↑の箇所のように文字間隔を空けて表記している部分は、【Space】キーを 1 回押してください。
また、上記のようなコマンド入力を英小文字で表記していますが、英大文字で入力してもかまいません。

・CD/DVD ドライブなどのドライブ名を、［CD/DVD ドライブ］で表記しています。入力の際は、お使いの環境に合わせて、ドライブ名を入力してください。

例：[CD/DVD ドライブ]:¥setup.exe

## ■連続する操作の表記

本文中の操作手順において、連続する操作手順を、「→」でつなげて記述しています。

例：「スタート」ボタンをクリックし、「すべてのプログラム」をポイントし、「アクセサリ」をクリックする操作

↓

「スタート」ボタン→「すべてのプログラム」→「アクセサリ」の順にクリックします。

また、本文中の操作手順において、操作手順の類似しているものは、あわせて記述しています。

## ■画面例およびイラストについて

表記されている画面およびイラストは一例です。お使いの機種や OS、Web ブラウザなどの環境、またインストールされている認証デバイスによって、画面およびイラストが若干異なることがあります。

## ■製品の呼び方

本文中の製品名称を、次のように略して表記します。

<table>
<tr><th>製品名称</th><th colspan="3">本文中の表記</th></tr>
<tr><td>認証デバイスを搭載した FMV シリーズ</td><td>パソコン本体</td><td colspan="2" rowspan="2">コンピュータ</td></tr>
<tr><td>認証デバイスを搭載した CELSIUS シリーズ</td><td>ワークステーション本体</td></tr>
<tr><td>FMV シリーズ内蔵スライド方式指紋センサー</td><td>指紋センサー</td><td colspan="2" rowspan="5">認証デバイス</td></tr>
<tr><td>FeliCa 対応リーダ／ライタ</td><td rowspan="3">リーダ／ライタ</td></tr>
<tr><td>スマートカードリーダ／ライタ</td></tr>
<tr><td>スマートカードホルダー</td></tr>
<tr><td>セキュリティチップ</td><td>セキュリティチップ</td></tr>
<tr><td>SMARTACCESS に対応した FeliCa 対応非接触 IC カード（FeliCa 対応非接触 IC カード（SMARTACCESS 専用）を含む）</td><td>IC カード（FeliCa 方式）</td><td colspan="2" rowspan="2">カード</td></tr>
<tr><td>スマートカード</td><td>スマートカード</td></tr>
<tr><td>SMARTACCESS/Basic</td><td colspan="3">SMARTACCESS</td></tr>
<tr><td>Windows Vista® Business</td><td>Windows Vista Business</td><td rowspan="5">Windows Vista</td><td rowspan="9">Windows</td></tr>
<tr><td>Windows Vista® Enterprise</td><td>Windows Vista Enterprise</td></tr>
<tr><td>Windows Vista® Ultimate</td><td>Windows Vista Ultimate</td></tr>
<tr><td>Windows Vista® Home Premium</td><td>Windows Vista Home Premium</td></tr>
<tr><td>Windows Vista® Home Basic</td><td>Windows Vista Home Basic</td></tr>
<tr><td>Microsoft® Windows® XP Professional</td><td>Windows XP Professional</td><td rowspan="3">Windows XP</td></tr>
<tr><td>Microsoft® Windows® XP Home Edition</td><td>Windows XP Home Edition</td></tr>
<tr><td>Microsoft® Windows® XP Tablet PC Edition 2005</td><td>Windows XP Tablet PC Edition 2005</td></tr>
<tr><td>Microsoft® Windows Server® 2003, Enterprise Edition</td><td>Windows Server 2003</td><td>Windows Server</td></tr>
<tr><td>Active Directory®</td><td colspan="3">Active Directory</td></tr>
<tr><td>Microsoft® Outlook® Express</td><td colspan="3">Outlook Express</td></tr>
<tr><td>Microsoft® Office Outlook®</td><td colspan="3">Outlook</td></tr>
<tr><td>Microsoft® Office Word</td><td colspan="3">Word</td></tr>
</table>

# 商標および著作権について

第 1 章

# お使いになる前に

認証デバイスや SMARTACCESS をお使いになる前に確認していただくことを説明しています。

# SMARTACCESS とは

コンピュータのセキュリティ対策の一つとして、重要な個人認証を強化する機能を提供するソフトウェアです。
対応する認証デバイスは次のとおりです。

- 指紋センサー
- スマートカードリーダ／ライタ
- セキュリティチップ
- FeliCa 対応リーダ／ライタ
- スマートカードホルダー

**重要**

- カスタムメイドで選択していない場合など、機種によってはお使いになれない認証デバイスもあります。

Windows やソフトウェアなどへのログオン時の ID やパスワードのキーボード入力を認証デバイスで代行し、安全かつ簡単にログオンすることができます。また、異なる認証デバイスを組み合わせせることにより、認証を強化することもできます。

従　来

BIOS
スマートカード
認証連携

BIOS
指紋認証
認証連携

電 源 O N

BIOSパスワード

パスワード直接入力

＊＊＊＊＊

スマートカード認証

指 紋 認 証

Windowsログオン

パスワード直接入力

指紋・ICカードによる認証

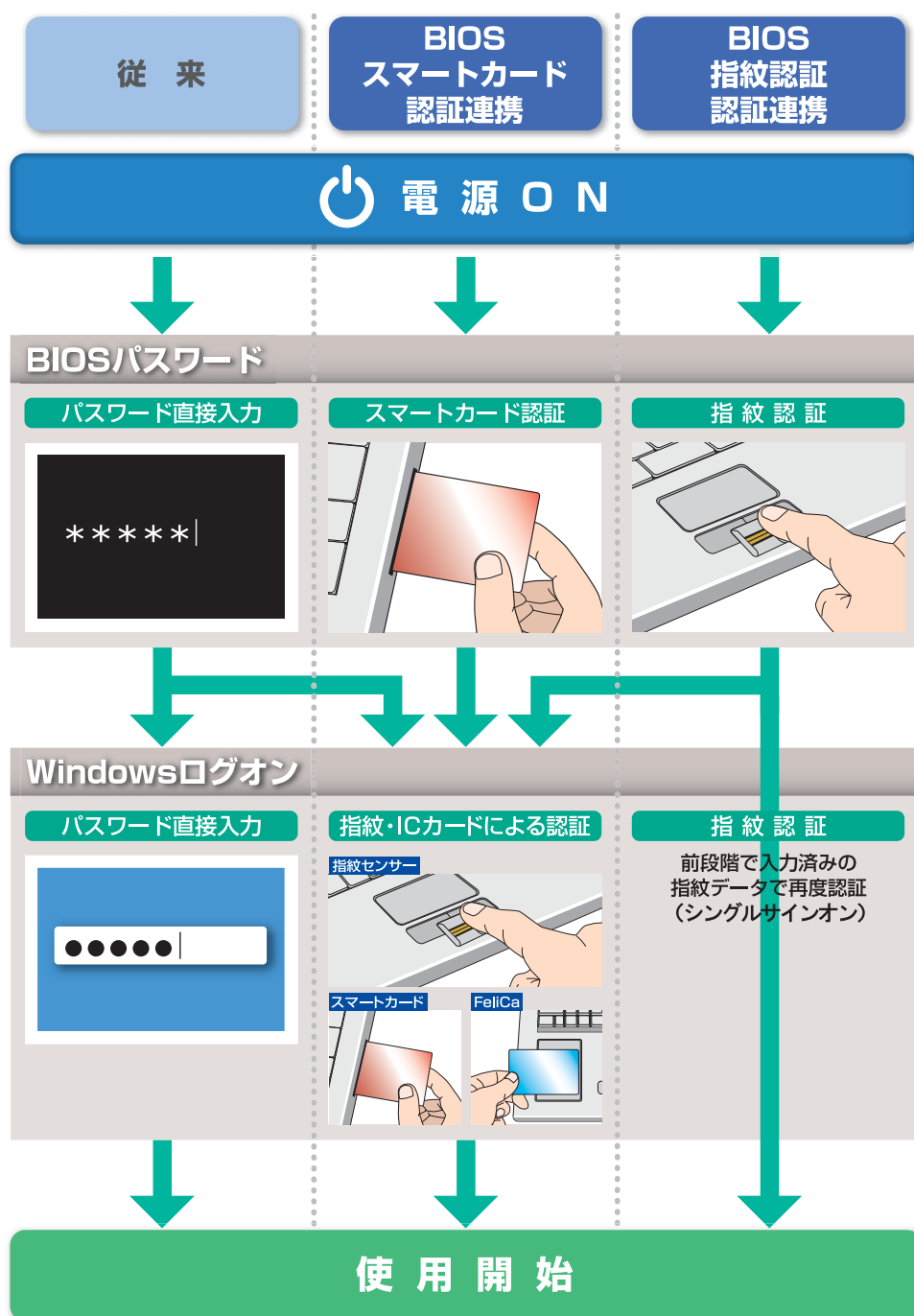
指紋センサー

スマートカード

FeliCa

指 紋 認 証

前段階で入力済みの
指紋データで再度認証
（シングルサインオン）

使 用 開 始

### □Windows へのログオン
IC カード（FeliCa 方式）やスマートカード、セキュリティチップ内に格納したログオン情報を利用して、Windows にログオンすることができます。またログオン情報のキーボード入力を指紋認証で代行することもできます。
この機能を使うと、コンピュータのロックの解除、スクリーンセーバーからの復帰時にも認証デバイスが必要になります。これにより離席時などにコンピュータを不正利用されるのを防ぐことができます。
また、複数の認証デバイスを組み合わせてログオン認証を行うことができます。

### □複数アプリケーションへのシングルサインオン
IC カード（FeliCa 方式）やスマートカード、セキュリティチップ内に格納したログオン情報を利用し、ソフトウェアへのログオンができます。またログオン情報のキーボード入力を指紋認証で代行することもできます。
ソフトウェアの認証画面を改造することなく、安価にシングルサインオン環境を導入することができます。

## 運用形態

SMARTACCESS の主な運用形態は次のとおりです。

### □1 台のコンピュータで管理者と利用者が同一の運用
導入から環境の設定、利用するまでを一括して一人で行います。主に個人ユーザーが利用する場合の運用形態です。

### □1 台のコンピュータで管理者と利用者が異なる運用
導入から環境の設定まで、一連の構築を管理者が行います。利用者は管理者が構築した環境で SMARTACCESS を利用します。

### □1 台のコンピュータを複数の利用者が使う運用
共有端末などを複数の利用者が使う場合、導入から利用者ごとの環境の設定までを管理者が行います。利用者は利用者ごとに設定された環境で SMARTACCESS を利用します。

# 2 動作環境

認証デバイスや SMARTACCESS をお使いになる前に、次の条件を確認してください。

重要

- カスタムメイドで選択していない場合など、機種によってはお使いになれない認証デバイスもあります。

## ■対応機種／ OS

認証デバイスが搭載されている FMV シリーズ、CELSIUS シリーズ／ Windows Vista、Windows XP
ハードディスク容量に 50MB 以上の空きがあること

## ■注意事項

・リモートデスクトップおよびリモート操作製品を使ったリモートでのログオン、ログオフには対応しておりません。

## ■SMARTACCESS がサポートする認証デバイス

| 認証デバイス | 製品名 |
|---|---|
| 指紋センサー | FMV シリーズ内蔵スライド方式指紋センサー |
| FeliCa 対応リーダ／ライタ | FMV-LIFEBOOK 内蔵の FeliCa 対応リーダ／ライタ |
| スマートカードリーダ／ライタ | FMV シリーズ、および CELSIUS シリーズ内蔵のスマートカードリーダ／ライタ |
| スマートカードホルダー | FMV-LIFEBOOK に添付のスマートカードホルダー |
| セキュリティチップ | FMV シリーズ、および CELSIUS シリーズ内蔵のセキュリティチップ |

## ■連携可能なソフトウェア

・Portshutter

対応バージョンは、コンピュータ本体に添付の「ドライバーズディスク」の「¥Security¥SABasic¥Readme.txt」をご覧ください。

## 第 2 章

# 機能概要

認証デバイスとSMARTACCESSを使った代表的な機能を説明しています。

# 代表的な機能の一覧

認証デバイスと SMARTACCESS を使った代表的な機能は次のとおりです。

○：対応　－：非対応

| 機能 | | 対応する認証デバイス | | | |
|---|---|---|---|---|---|
| | | 指紋センサー | FeliCa 対応リーダ／ライタ | スマートカードリーダ／ライタ<br>スマートカードホルダー | セキュリティチップ |
| 不正使用対策 | 「Windows やソフトウェアなどへのログオン時の認証」（→ P.13） | ○ | ○ | ○ | ○ |
| | 「BIOS パスワードとの連携」（→ P.13） | ○注 1 | – | ○注 1 | – |
| | 「カード操作によるコンピュータのロック」（→ P.14） | – | ○ | ○ | – |
| 情報漏えい対策 | 「Windows 暗号化ファイルシステム（EFS）の鍵の保護」（→ P.14） | – | – | – | ○ |
| | 「不正なハードウェアの変更の検出（機器監査機能）」（→ P.14） | – | – | – | ○ |
| | 「「Portshutter」との連携」（→ P.14） | ○ | ○ | ○ | ○ |
| 運用管理機能 | 「利用ログ管理」（→ P.15） | ○ | ○ | ○ | ○ |
| | 「SMARTACCESS の設定のバックアップ」（→ P.15） | ○ | ○ | ○ | ○ |

注 1：BIOS パスワードとの連携機能に対応しているコンピュータでお使いになれます。

# 2 代表的な機能の紹介

## 不正使用対策

### ■Windows やソフトウェアなどへのログオン時の認証

#### □対応する認証デバイス

・指紋センサー
・FeliCa 対応リーダ／ライタ
・スマートカードリーダ／ライタ、スマートカードホルダー
・セキュリティチップ

Windows の起動時や、ユーザー名とパスワードで運用している Web サイトやソフトウェアにログオンするときに、セキュリティチップやカードに格納したログオン情報、または指紋を読み取ることによってログオンすることができます。
複数の異なる認証デバイスを組み合わせてお使いになることもできます。
例えば、セキュリティチップと指紋センサーを組み合わせると、セキュリティチップに格納したログオン情報のパスワード入力を指紋認証で代行することができ、パスワードを入力するだけの認証よりもさらにセキュリティが高まります。

**・Windows ログオン機能**

Windows の起動時やコンピュータのロック解除時、休止状態からの復帰時、スクリーンセーバーからの復帰時に、認証デバイスを使ってログオンすることができます。
設定方法などについては、「設定」（→ P.31）をご覧ください。

**・アプリケーションログオン機能**

ユーザー名とパスワードで運用している Web サイトやソフトウェアなどに、認証デバイスを使ってログオンすることができます。
詳しくは、『リファレンスガイド』の「機能編」－「ログオン認証」－「アプリケーションログオン」をご覧ください。

**・シングルサインオン**

通常は Windows やソフトウェアへのログオンごとに認証を行う必要がありますが、シングルサインオン機能をお使いになると、一度ログオン認証に成功すれば以降は同一のユーザーがコンピュータを継続して使っているものとして、ログオン認証を省略することができます。
ただし次の場合は、再度認証の必要があります。
- Windows を終了した場合、またはユーザーの切り替えやログオフをしたとき
- コンピュータがロックされたとき
- Windows のパスワードを変更したとき

また、SMARTACCESS の「環境設定」や「ユーザー情報設定」の起動はシングルサインオン機能の対象外です。
詳しくは、『リファレンスガイド』の「機能編」－「ログオン認証」－「シングルサインオン機能」をご覧ください。

### ■BIOS パスワードとの連携

#### □対応する認証デバイス

・指紋センサー
・スマートカードホルダー

コンピュータの不正使用を防止するための BIOS のパスワード機能を、指紋情報やスマートカードと組み合わせて使用することができます。コンピュータの起動時やスタンバイからレジュームするときに、キーボードから BIOS パスワードを入力する代わりに、指紋の読み取りやスマートカードをセットすることで認証する機能です。
この機能は、BIOS パスワードとの連携機能に対応しているコンピュータでお使いになれます。
指紋センサーの場合、BIOS の認証をすれば Windows ログオン時の認証を省略できる「シングルサインオン」機能を使うこともできます。
設定方法などについては、「設定」（→ P.31）をご覧ください。

### ■カード操作によるコンピュータのロック

#### □対応する認証デバイス

・FeliCa 対応リーダ／ライタ
・スマートカードリーダ／ライタ、スマートカードホルダー

スマートカードや IC カード（FeliCa 方式）をリーダ／ライタにセットした状態から外したり、リーダ／ライタにタッチしたりすることによって、コンピュータをロックしたりシャットダウンしたりすることができます。離席時などにコンピュータの不正利用を防ぐための機能です。
設定方法などについては、「設定」（→ P.31）をご覧ください。

## 情報漏えい対策

### ■Windows 暗号化ファイルシステム（EFS）の鍵の保護

#### □対応する認証デバイス

・セキュリティチップ

Windows 暗号化ファイルシステム（EFS）と連携し、暗号鍵を管理します。暗号化されたデータは暗号鍵がない限り復元できないため、ハードディスクドライブごと盗難に遭ってもデータを読み込むことができません。
詳しくは、『リファレンスガイド』の「機能編」－「ファイルセキュリティ」－「セキュリティチップによる Windows 暗号化ファイルシステム（EFS）の鍵の保護」をご覧ください。

### ■不正なハードウェアの変更の検出（機器監査機能）

#### □対応する認証デバイス

・セキュリティチップ

コンピュータの電源を入れた直後の Windows へのログオン時にコンピュータの機器構成のチェックを行い、ハードウェア構成または設定が不正に変更されていることを検出した場合に、警告を表示したり、Windows ログオンを拒否したりすることができます。
これにより、離席中など気付かないうちにハードウェアを変更されても、検出することができます。
なお、不正にコンピュータの設定が変更されたときだけでなく、修理により設定が変更された場合にも変更が検出されることがあります。修理に出す前に「コンピュータの修理や保守を依頼する場合」（→ P.98）をご覧になり、設定を変更できるようにしてください。
検出できるハードウェア構成の変更は次のとおりです。

・BIOS のハードウェア構成
・メモリスロットの構成
・USB ポートに、USB メモリなどのストレージデバイスを接続したとき
・PCI スロットの構成、およびグラフィックボード（FMV-ESPRIMO シリーズ、FMV ロングライフパソコン、および CELSIUS シリーズ）
・モバイルマルチベイ、およびマルチベイ（FMV-LIFEBOOK シリーズ）

詳しくは、『リファレンスガイド』の「機能編」－「ログオン認証」－「機器監査」をご覧ください。

### ■「Portshutter」との連携

#### □対応する認証デバイス

・指紋センサー
・FeliCa 対応リーダ／ライタ
・スマートカードリーダ／ライタ、スマートカードホルダー
・セキュリティチップ

USB ポートや CD/DVD ドライブなどの外部機器接続ポートの使用を制限することにより、コンピュータからの情報漏洩やコンピュータへの不正なプログラムの導入を防ぐことができるソフトウェア「Portshutter」をお使いの場合、SMARTACCESS の「環境設定」から「Portshutter」の管理者ツールを起動したり、管理者パスワードを変更したりすることができます。
詳しくは、『リファレンスガイド』の「機能編」－「機器制限」をご覧ください。

# 運用管理機能

## ■利用ログ管理

### □対応する認証デバイス

・指紋センサー
・FeliCa 対応リーダ／ライタ
・スマートカードリーダ／ライタ、スマートカードホルダー
・セキュリティチップ

システムで発生したエラーや警告などのログ情報をログファイルに格納することにより、コンピュータ上で不正アクセスの原因や利用状況などを追跡できます。
詳しくは、『リファレンスガイド』の「機能編」－「利用ログ」をご覧ください。

## ■SMARTACCESS の設定のバックアップ

### □対応する認証デバイス

・指紋センサー
・FeliCa 対応リーダ／ライタ
・スマートカードリーダ／ライタ、スマートカードホルダー
・セキュリティチップ

SMARTACCESS の環境設定情報やユーザー情報のバックアップファイルを作成しておき、ファイル装置や認証デバイスなどの障害によって環境設定情報やユーザー情報を損失した場合に復元できます。
詳しくは、『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧ください。

## 第 3 章

# インストール

インストールからお使いになるまでの基本的な流れと、インストール手順について説明しています。

# 1 インストールと設定の流れ

導入の手順は、お使いになる認証デバイスや機能によって異なります。インストールと設定の基本的な流れは次のとおりです。

## □用意するもの

・パソコンまたはワークステーション本体
・ドライバーズディスク

●必須　○お使いになる機種や機能によって設定　×該当機能なし　ー設定不要

| 項目 | 指紋センサー | Felica 対応リーダ／ライタ | スマートカードリーダ／ライタ<br>スマートカードホルダー | セキュリティチップ |
|---|---|---|---|---|
| **認証デバイスのインストール** | | | | |
| BIOS の確認 | ― | ●注 1 | ― | ●注 1 |
| ドライバのインストール | ● P.19 | ● P.19 | ● P.19 | ● P.19 |

| 項目 | 指紋センサー | Felica 対応リーダ／ライタ | スマートカードリーダ／ライタ<br>スマートカードホルダー | セキュリティチップ |
|---|---|---|---|---|
| SMARTACCESS のインストール | ● P.23 | ● P.23 | ● P.23 | ● P.23 |

| 項目 | 指紋センサー | Felica 対応リーダ／ライタ | スマートカードリーダ／ライタ<br>スマートカードホルダー | セキュリティチップ |
|---|---|---|---|---|
| **管理者による設定** | | | | |
| 認証パターンの設定 | ● P.36 | ● P.54 | ● P.64 | ● P.77 |
| SMARTACCESS アカウント | ● P.38 | ● P.56 | ● P.66 | ● P.79 |
| Windows ログオン機能の設定 | ○ P.48 | ○ P.60 | ○ P.70 | ○ P.82 |
| BIOS パスワードとの連携機能の設定 | ○ P.51 注 2 | × | ○ P.74 注 2 | × |
| カード操作によるコンピュータのロック機能の設定 | × | ○ P.60 | ○ P.71 | × |

| 項目 | 指紋センサー | Felica 対応リーダ／ライタ | スマートカードリーダ／ライタ<br>スマートカードホルダー | セキュリティチップ |
|---|---|---|---|---|
| **利用者による設定** | | | | |
| 指紋の登録 | ● P.42 | × | × | × |
| パスワードの変更 | ● P.49 | ● P.61 | ● P.72 | ● P.83 |

注 1：参照先は、コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」
注 2：コンピュータ本体の BIOS セットアップで、BIOS セットアップの起動時にパスワードの認証が必要となるように設定する必要があります。

# 2 認証デバイスのインストール

SMARTACCESS をインストールする前に、お使いになる認証デバイスのドライバやユーティリティソフトのインストールが必要です。SMARTACCESS では、複数の認証デバイスを組み合わせて利用することもできます。

## BIOS の設定を確認する

次の認証デバイスをお使いになる場合、認証デバイスのドライバやユーティリティソフトをインストールする前に必ず BIOS の設定を確認してください。
・FeliCa 対応リーダ／ライタ
・セキュリティチップ

### □FeliCa 対応リーダ／ライタをお使いになる場合

コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧になり、BIOS の設定を確認してください。

### □セキュリティチップをお使いになる場合

コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧になり、BIOS の設定を変更してください。

## 認証デバイスのインストール

**1 管理者権限をもつアカウントで Windows にログオンします。**

**2 使用中のソフトウェアをすべて終了させます。**

**3 それぞれの認証デバイスの「Readme.txt」をご覧になり、認証デバイスのドライバやユーティリティソフトをインストールします。**

「Readme.txt」は、コンピュータ本体に添付の「ドライバーズディスク」に格納されています。
格納先フォルダは次のとおりです。

| 認証デバイス | 格納先フォルダ |
|---|---|
| 指紋センサー（FMV-LIFEBOOK） | ¥Security¥fingerprint |
| FeliCa 対応リーダ／ライタ | ¥Security¥SONY FeliCa リーダー _ ライター |
| スマートカードリーダ／ライタ<br>（FMV-ESPRIMO、CELSIUS シリーズ） | ¥Security¥Smart |
| スマートカードホルダーまたは<br>スマートカードスロット（FMV-LIFEBOOK） | ¥Security¥O2scb |
| セキュリティチップ | ¥Security¥IFXSW30 |

### □スマートカードをお使いになる場合

ドライバのインストール後に、次の手順でスマートカードの設定を確認してください。

**1 「スタート」ボタン→「コントロールパネル」の順にクリックします。**

「コントロールパネル」ウィンドウが表示されます。

## 2 次の操作をします。

■ Windows Vista の場合

「システムとメンテナンス」→「管理者ツール」の順にクリックします。

■ Windows XP の場合

「パフォーマンスとメンテナンス」→「管理ツール」の順にクリックします。

「管理ツール」ウィンドウが表示されます。

## 3 「サービス」をダブルクリックします。

■ Windows Vista をお使いの場合

「ユーザーアカウント制御」ウィンドウが表示された場合は、「続行」をクリックします。

「サービス」ウィンドウが表示されます。

## 4 「Smart Card」の「スタートアップの種類」が「自動」になっていることを確認します。

「スタートアップの種類」が「自動」になっていない場合は次の手順に進みます。

「自動」になっている場合は、確認はこれで完了です。

## 5 「Smart Card」をダブルクリックします。

「(ローカル コンピュータ) Smart Card のプロパティ」ウィンドウが表示されます。

## 6 「全般」タブの「スタートアップの種類」から「自動」を選択します。

## 7 「サービスの状態」の「開始」をクリックします。

## 8 「OK」をクリックし、すべてのウィンドウを閉じます。

#  SMARTACCESS のインストール

## SMARTACCESS をインストールする前に

・次の製品がインストールされている場合、SMARTACCESS をインストールする前に必ずアンインストールしてください。
- SMARTACCESS/Trust
- SMARTACCESS/Feel
- SMARTACCESS/BASE
- SMARTACCESS/PRO
- Secure Login Light
- Secure Login Client
- Softex OmniPass

上記製品以外でも、Windows ログオン認証を行うソフトウェアと SMARTACCESS を併用することはできません。SMARTACCESS をインストールする前に、必ず他の Windows ログオン認証ソフトウェアをアンインストールしてください。

**重要**

▶ 旧バージョンの SMARTACCESS や、Secure Login Light などのアンインストールは次の手順で行います。
1. 「スタート」ボタン→「コントロールパネル」の順にクリックします。
「コントロールパネル」ウィンドウが表示されます。
2. 次の操作を行います。
・Windows Vista の場合
「プログラムのアンインストール」をクリックします。
・Windows XP の場合
「プログラムの追加と削除」をクリックします。
3. アンインストールする製品を選択し、削除します。
再起動の要求があった場合は、必ず再起動を行ってください。

・お使いになる認証デバイスのインストールが完了してから、SMARTACCESS をインストールしてください。SMARTACCESS をインストールした後に認証デバイスをインストールすると、認証デバイスが正常に認識されません。
・ハードディスクに十分な空き容量（→ P.10）があることを確認してください。

### □Windows Vista で FeliCa 対応リーダ／ライタのグローバルカード管理リストをお使いになる場合

Windows で「ネットワーク探索」を有効にしておく必要があります。
SMARTACCESS をインストールする前に、ネットワークに接続した状態で次の手順を設定してください。
グローバル管理リストについては『リファレンスガイド』の「機能編」－「カード管理」－「カード管理リスト」をご覧ください。

**1** 「スタート」ボタン→「コントロールパネル」の順にクリックします。

**2** 「ネットワークとインターネット」をクリックします。

**3** 「ネットワークと共有センター」をクリックします。

**4** 「共有と探索」の「ネットワーク探索」をクリックします。

**5** 「ネットワーク探索を有効にする」をクリックします。

**6** 「適用」をクリックします。

### □Windows Vista で BitLocker ドライブ暗号化をお使いになる場合

認証デバイスとしてセキュリティチップを使用し、BitLockerドライブ暗号化をお使いになる場合は、SMARTACCESSのインストール前にあらかじめBitLockerドライブ暗号化を一時的に無効にし、BIOSでセキュリティチップをクリアしておく必要があります。
設定手順は次のとおりです。

**1 「スタート」ボタン→「コントロールパネル」の順にクリックします。**

「コントロールパネル」ウィンドウが表示されます。

**2 「セキュリティ」→「BitLocker ドライブ暗号化」の順にクリックします。**

「BitLocker ドライブ暗号化」ウィンドウが表示されます。

**3 次の操作をします。**

- **回復パスワードがない場合**
  「BitLocker キーの管理」をクリックして画面の指示に従います。
- **回復パスワードがある場合**
  手順 4 に進みます。

**重要**

- セキュリティチップのクリアを行う前に、保存済みの BitLocker の回復パスワードをご用意ください。回復パスワードがない場合、必ず回復パスワードの複製を作成してください。
  回復パスワードについては Windows のヘルプをご覧ください。

**4 「BitLocker をオフにする」をクリックします。**

「BitLocker ドライブ暗号化」ウィンドウが表示されます。

**5 「BitLocker ドライブ暗号化を無効にします」をクリックします。**

**6 コンピュータを再起動し、BIOS でセキュリティチップのクリアを行います。**

セキュリティチップのクリアについては、コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧ください。

**POINT**

- BIOS でセキュリティチップをクリアすると、Windows でセキュリティチップ（TPM）を初期化するときに作成する「TPM 所有者バックアップファイル」はお使いになれません。

SMARTACCESS のインストール後、BitLocker をオンにすることで BitLocker ドライブ暗号化が再度有効になります。

## インストールの権限について

SMARTACCESS をインストールするには、管理者権限を持つ Windows アカウントである必要があります。それ以外の権限ではインストールしないでください。
運用形態とインストールする管理者権限の関係は、次のとおりです。

| 運用形態 | 必要とする権限 |
|---|---|
| スタンドアロンまたはワークグループ環境 | ローカルコンピュータの Administrators グループのメンバー |
| ドメイン環境 | Active Directory（ドメインコントローラ）の Domain Admins グループのメンバー |

# SMARTACCESS のインストール

お使いになる認証デバイスのインストールが完了してから、SMARTACCESS をインストールしてください。SMARTACCESS をインストールした後に認証デバイスをインストールすると、認証デバイスが正常に認識されません。
インストールの手順は次のとおりです。

## 1 コンピュータを起動し、管理者権限を持つアカウント（→ P.22）で Windows にログオンします。

■ スマートカードホルダーをお使いになる場合
コンピュータの電源を入れる前に、スマートカードホルダーをセットします。
スマートカードホルダーのセットのしかたについては、「認証デバイスの取り扱い」－「スマートカードリーダ／ライタ、スマートカードホルダー」－「取り扱い方」（→ P.92）をご覧ください。

## 2 使用中のソフトウェアをすべて終了させます。

## 3 コンピュータ本体に添付の「ドライバーズディスク」をセットします。

## 4 次の操作をします。

■ Windows Vista の場合
「スタート」ボタン→「すべてのプログラム」→「アクセサリ」→「ファイル名を指定して実行」の順にクリックします。

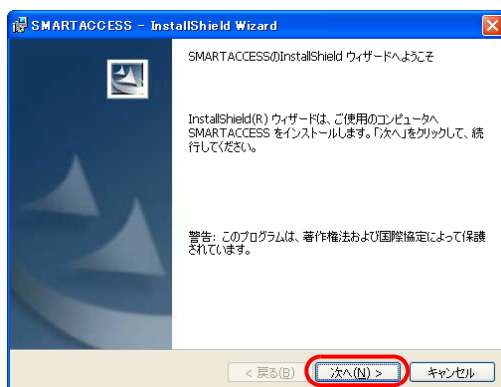
■ Windows XP の場合
「スタート」ボタン→「ファイル名を指定して実行」の順にクリックします。

## 5 「名前」に次のように入力し、「OK」をクリックします。

［CD/DVD ドライブ］:¥Security¥SABasic¥Setup¥setup.exe

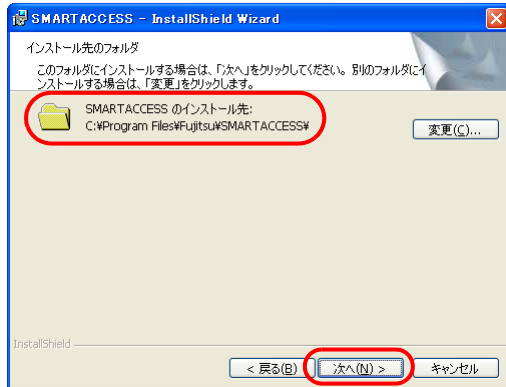
■ Windows Vista の場合
「ユーザーアカウント制御」ウィンドウが表示された場合は、開始されるプログラムを確認し、「続行」をクリックします。
「SMARTACCESS 用の InstallShied ウィザードへようこそ」と表示されます。

■ Windows XP の場合
「SMARTACCESS 用の InstallShied ウィザードへようこそ」と表示されます。

## 6 「次へ」をクリックします。

「インストール先のフォルダ」が表示されます。

## 7 インストール先を確認し、「次へ」をクリックします。

インストール先を変更する場合は、「変更」をクリックします。

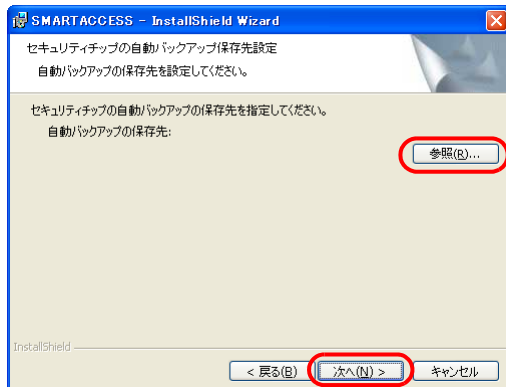
**重要**

- セキュリティチップをお使いになる場合、システムフォルダのあるドライブと、SMARTACCESS のインストール先ドライブは同じ場所にしてください。セキュリティチップが正常に使用できなくなる場合があります。

■ **セキュリティチップがインストールされている場合**

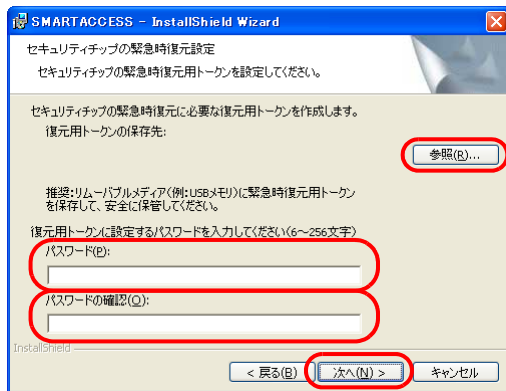
「セキュリティチップの自動バックアップ保存先設定」ウィンドウが表示されます。
手順 8 に進んでください。

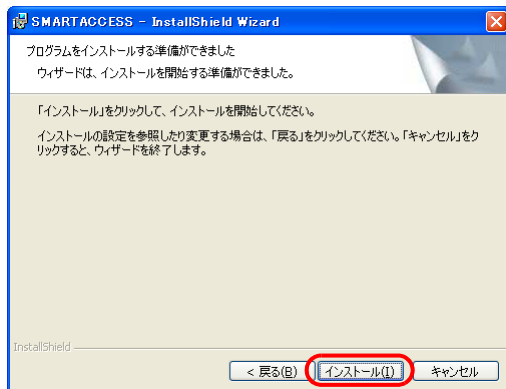
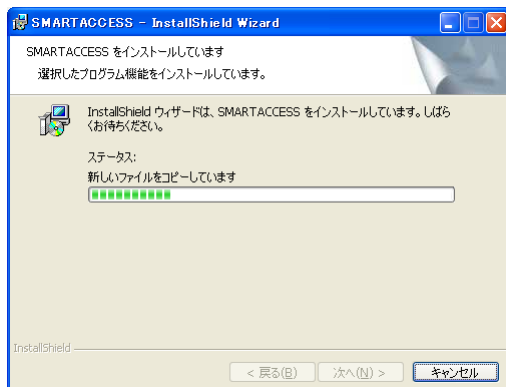
■ **セキュリティチップがインストールされていない場合**

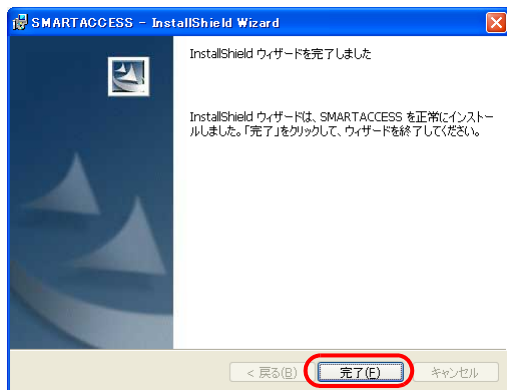
「プログラムをインストールできる準備ができました」と表示されます。
手順 11 に進んでください。

## 8 「参照」をクリックして、自動バックアップの保存先を指定し、「次へ」をクリックします。

「セキュリティチップの緊急時復元設定」ウィンドウが表示されます。

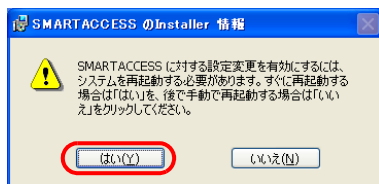
## 9 「参照」をクリックして、復元用トークンの保存先を指定します。

## 10 「パスワード」と「パスワードの確認」に、復元用トークンに設定するパスワードを 6 文字以上 256文字以下で入力し、「次へ」をクリックします。

「プログラムがインストールできる準備ができました」と表示されます。

## 11 「インストール」をクリックして、インストールを開始します。

「SMARTACCESS をインストールしています」と表示されます。

インストールが正常に完了すると、「InstallShield ウィザードを完了しました」と表示されます。

### 12 「完了」をクリックします。

インストールの完了後に、「コマンドプロンプト」ウィンドウが表示されることがあります。「コマンドプロンプト」ウィンドウは自動的に閉じますので手動で終了しないでください。
「SMARTACCESS の InstallShield 情報」メッセージが表示されます。

### 13 「はい」をクリックして、コンピュータを再起動します。

**重要**

- セキュリティチップをお使いになる場合、SMARTACCESS インストール後に「最近使ったファイル」の一覧に、自動バックアップの保存先で指定したファイルと復元用トークンの保存先で指定したファイルが追加されることがありますが、選択しないでください。

**□過去にお使いになっていた SMARTACCESS の設定情報を再利用する場合**

過去に SMARTACCESS をお使いになっていて、使用していた設定情報やセキュリティチップの鍵や証明書などを再利用する場合は、アンインストール前にバックアップしておいた設定情報(→ P.28)をリストアしてください。リストアの手順については、『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧ください。

## 認証デバイスの追加

何らかの認証デバイスと SMARTACCESS をすでにお使いの環境に、さらに別の認証デバイスを追加する場合、新たな認証デバイスのドライバをインストールする前に SMARTACCESS をいったんアンインストールする必要があります。

### 1 「バックアップツール」で、環境設定情報や全ユーザーのデータを退避します。

「バックアップツール」については、『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧ください。

### 2 SMARTACCESS をアンインストールします。

アンインストールの手順などについては、「アンインストール」－「SMARTACCESS のアンインストール」（→ P.28）をご覧ください。

### 3 追加する認証デバイスのドライバやユーティリティソフトをインストールします。

インストールの手順などについては、「認証デバイスのインストール」（→ P.19）をご覧ください。

**4** **SMARTACCESS をインストールします。**

インストールの手順などについては、「SMARTACCESS のインストール」（→ P.23）をご覧ください。

**5** **「バックアップツール」で、環境設定情報や全ユーザーのデータを復元します。**

詳しくは、『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」－「バックアップファイルの復元」をご覧ください。

**6** **「認証パターン」を設定し直します。**

「バックアップツール」で環境設定情報などを復元すると、「認証パターン」の設定は前の環境の設定が引き継がれるため、追加した認証デバイスをそのまま使用することはできません。
「認証パターン」の設定については、『リファレンスガイド』の「機能編」－「ログオン認証」－「認証パターンの設定」をご覧ください。

## 認証デバイスの削除

使用中の認証デバイスの一部をアンインストールする場合、SMARTACCESS をインストールし直す必要があります。

**1** **「環境設定」で「SMARTACCESS による Windows ログオン」が「しない」になっていることを確認します。**

「SMARTACCESS による Windows ログオン」が「する」になっている場合は、「しない」にし、「OK」をクリックして必ずコンピュータを再起動してください。

**2** **「バックアップツール」で、環境設定情報や全ユーザーのデータを退避します。**

「バックアップツール」については、『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧ください。

**3** **SMARTACCESS をアンインストールします。**

アンインストールの手順などについては、「SMARTACCESS のアンインストール」（→ P.28）をご覧ください。

**4** **認証デバイスのドライバやユーティリティソフトをアンインストールします。**

アンインストールの手順などについては、「認証デバイスのアンインストール」（→ P.29）をご覧ください。

**5** **SMARTACCESS をインストールします。**

インストールの手順などについては、「SMARTACCESS のインストール」（→ P.23）をご覧ください。

**6** **「バックアップツール」で、環境設定情報や全ユーザーのデータを復元します。**

詳しくは、『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」－「バックアップファイルの復元」をご覧ください。

# 4 アンインストール

## SMARTACCESS のアンインストール

### ■SMARTACCESS をアンインストールする前に

・「環境設定」で「SMARTACCESS による Windows ログオン」が「しない」になっていることを確認してください。
「SMARTACCESS による Windows ログオン」が「する」になっている場合は、「しない」にし、「適用」または「OK」をクリックして、コンピュータを必ず再起動してください。再起動を行わないと、設定した内容が有効になりません。
・暗号化したファイルやメールなどがある場合は、暗号化を解除してからアンインストールを行ってください。
・パスワードの自動生成を行っている場合は、いったん「パスワードの自動生成」を「しない」にした後、お使いの認証デバイスの「パスワードの変更」のページにある手順で任意のパスワードに変更してからアンインストールを行ってください。
「パスワードの自動生成」については『リファレンスガイド』の「機能編」－「ログオン認証」－「Windows ログオン」－「パスワードの自動生成」をご覧ください。

#### □SMARTACCESS の設定情報を再利用する場合

認証デバイスの追加や削除などにより SMARTACCESS をアンインストールしてから再び SMARTACCESS をお使いになる場合、必ず SMARTACCESS の設定情報をバックアップしてください。
バックアップしておかないと、使用していた SMARTACCESS の設定情報や、セキュリティチップの鍵、証明書を再利用できなくなります。
バックアップの手順については、『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧ください。

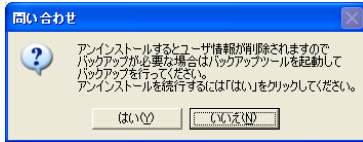
### ■SMARTACCESS のアンインストール

SMARTACCESS のアンインストールは、インストールを行ったユーザーのみ行うことができます。

**1** **SMARTACCESS をインストールしたのと同じアカウントで Windows にログオンします。**

**2** **「スタート」ボタン→「コントロールパネル」の順にクリックします。**
「コントロールパネル」ウィンドウが表示されます。

**3** **次の操作をします。**
■ Windows Vista の場合
1.「プログラムのアンインストール」をクリックします。
2.「SMARTACCESS」をクリックし、「アンインストール」をクリックします。
「SMARTACCESS をアンインストールしますか？」と表示されます。
3.「はい」をクリックします。
4.「ユーザーアカウント制御」ウィンドウが表示された場合は、開始されるプログラムを確認し、「許可」をクリックします。
■ Windows XP の場合
1.「プログラムの追加と削除」をクリックします。
2.「SMARTACCESS」をクリックし、「削除」をクリックします。
「このコンピュータから SMARTACCESS を削除しますか？」と表示されます。
3.「はい」をクリックします。
バックアップについての問い合わせメッセージが表示されます。

### 4 次の操作をします。

■ SMARTACCESS の設定やユーザー情報のバックアップを行う場合
「いいえ」をクリックしていったん SMARTACCESS のアンインストールを中止します。
「バックアップツール」でバックアップをしてから、再度 SMARTACCESS のアンインストールをしてください。
なお「いいえ」をクリックすると「致命的なエラー」というメッセージが表示されますが、問題はありません。
「OK」をクリックしてください。

■ SMARTACCESS の設定やユーザー情報のバックアップを行わない場合
「はい」をクリックします。SMARTACCESS の設定やユーザー情報は削除されます。

この後は、メッセージに従って操作します。
再起動を要求するメッセージが表示された場合は、必ず再起動を行ってください。

**POINT**

- SMARTACCESSがインストール済みの環境でSMARTACCESSの「setup.exe」を実行した場合も、アンインストールが開始されます。

### □セキュリティチップをお使いの場合

認証デバイスの追加や削除などにより SMARTACCESS をアンインストールした後、再びセキュリティチップを使用して SMARTACCESS をお使いになる場合、SMARTACCESS のアンインストール後に必ず次のことをしてください。

### 1 Security Platform（Infineon TPM ProfessionalPackage）をアンインストールします。

Security Platform（Infineon TPM ProfessionalPackage）のアンインストールについては「認証デバイスのアンインストール」（→ P.29）、およびセキュリティチップの「Readme.txt」（→ P.19）をご覧ください。

### 2 BIOS セットアップでセキュリティチップのクリアをします。

## 認証デバイスのアンインストール

認証デバイスのドライバのアンインストールは、次のとおり行います。

- Windows Vista をお使いの場合
  「コントロールパネル」→「プログラムのアンインストール」
- Windows XP をお使いの場合
  「コントロールパネル」→「プログラムの追加と削除」
  詳しくは、それぞれの認証デバイスの「Readme.txt」（→ P.19）をご覧ください。

### ■アンインストール時の注意事項

- 認証デバイスのドライバをアンインストールする場合は、必ず SMARTACCESS をアンインストールしてからドライバのアンインストールを行ってください。
  認証デバイスのドライバをアンインストールした状態で、SMARTACCESS によるログオンを行うと、Windows が正常に起動しなくなります。
- 複数の認証デバイスをお使いの場合に、一部の認証デバイスのドライバをアンインストールするときは、必ずいったん SMARTACCESS をアンインストールしてからドライバのアンインストールを行ってください。
  「認証デバイスの削除」については、「認証デバイスの削除」（→ P.27）をご覧ください。
- 認証デバイスのドライバをアンインストールするには、管理者権限でWindowsにログオンする必要があります。
- 再起動を要求するメッセージが表示された場合は、必ず再起動を行ってください。

第 4 章

# 設定

認証デバイスを使ってWindowsへのログオン時の認証を行うための設定について説明しています。

# SMARTACCESS の初期設定をする前に

インストールが終わった後、SMARTACCESS を起動する前に準備しておくこと、および知っておいていただきたいことを説明しています。

## SMARTACCESS での管理者と利用者

SMARTACCESS を使ったセキュリティ環境を構築する側を「管理者」、そのセキュリティ環境を利用する側を「利用者」と呼びます。
管理者は最適なセキュリティ環境を利用者に提供するための設定および管理を行い、利用者はそのセキュリティ環境により認証デバイスを利用してコンピュータに安全にアクセスすることができます。

管理者および利用者の権限は次のとおりです。

| | スタンドアロンまたはワークグループ環境 | ドメイン環境 |
|---|---|---|
| 管理者 | ローカルコンピュータのAdministratorsグループのメンバー | Active Directory（ドメインコントローラ）のDomain Adminsグループのメンバー |
| 利用者 | Usersグループのメンバー | Domain Usersグループのメンバー |

**□Windows Vista で指紋センサーをお使いの場合**

利用者をローカルコンピュータの Guests グループのメンバーに所属させないでください。認証に失敗します。

## Windows アカウントのパスワード設定

SMARTACCESS の管理者および利用者の Windows アカウントには、パスワードを設定する必要があります。
既存の Windows アカウントを SMARTACCESS で管理者アカウント、または利用者アカウントとしてお使いになる場合は、あらかじめ Windows でパスワードの設定をします。
また、SMARTACCESS で Windows アカウントを追加してパスワードを設定することもできます（→それぞれの認証デバイスの「アカウントの登録」）。
Windows のパスワード設定については、Windows のヘルプをご覧ください。

## スリープ／スタンバイからの復帰時のパスワード要求設定

コンピュータのセキュリティを高めるために、スリープ／スタンバイからの復帰時にパスワード入力を求めるように設定をします。

### ■Windows Vista をお使いの場合

1 **「スタート」ボタン→「コントロールパネル」の順にクリックします。**

2 **「システムとメンテナンス」→「電源オプション」の順にクリックします。**

3 **「スリープ解除時のパスワード保護」をクリックします。**

4 **「パスワードを必要とする（推奨）」に設定されていることを確認します。**
コンピュータご購入時の設定は「パスワードを必要とする」に設定されています。

### ■Windows XP をお使いの場合

**1** 「スタート」ボタン→「コントロールパネル」の順にクリックします。

**2** 「電源オプション」をクリックします。

**3** 「詳細設定」タブをクリックし、「スタンバイから回復するときにパスワードの入力を求める」にチェックをします。

## Windows XP の「共有とセキュリティ」をお使いの場合

Windows XP の「共有とセキュリティ」を使って、ユーザープロファイルのフォルダを「プライベート」に設定している場合は、ユーザープロファイルのフォルダへのアクセスは利用者のみに許可されます。
SMARTACCESS の設定を行うとき、管理者が利用者のユーザープロファイルのフォルダにアクセスする必要があることがありますので、「このフォルダをプライベートにする」の設定をオフにしてください。
設定をオフにする手順は次のとおりです。

**重要**

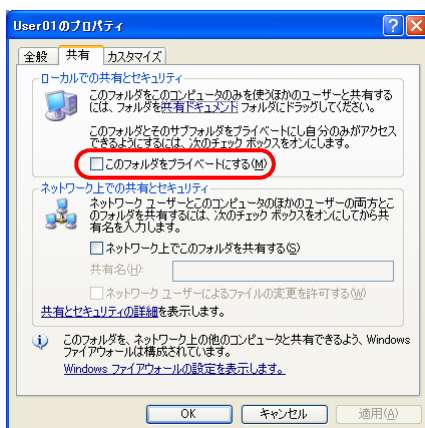
- 「このフォルダをプライベートにする」設定を変更するには、管理者権限をもつアカウントでログオンしている必要があります。
- ユーザープロファイルやフォルダのプライベート設定については、Windows のヘルプをご覧ください。

**1** 「スタート」ボタン→「マイコンピュータ」の順にクリックします。

「マイコンピュータ」ウィンドウが表示されます。

**2** Windowsがインストールされているドライブ(通常は「ローカル ディスク(C:)」)→「Document and Settings」の順にダブルクリックします。

**3** 設定を変更するユーザーアカウント名のフォルダを右クリックし、「共有とセキュリティ」をクリックします。

「[ユーザー名] のプロパティ」ウィンドウが表示されます。
「ローカルでの共有とセキュリティ」の「このフォルダをプライベートにする」のチェックを外します。

**4** 「OK」をクリックし、すべてのウィンドウを閉じます。

**重要**

- 運用上の都合などで「このフォルダをプライベートにする」をチェックしている場合、管理者は次の設定ができなくなります。
  ・「環境設定」－「ユーザー情報管理」の「アカウント追加」

・「環境設定」－「ユーザー情報管理」－「セキュリティチップ」の「ユーザー情報設定の起動」
・「ユーザー情報設定」

## ご購入時の設定について

認証デバイスには、ご購入時にユーザー名やパスワード、PIN があらかじめ設定されていますが、セキュリティ上、使い始めるときには必ずパスワードや PIN を変更してください。パスワードや PIN の変更については、『リファレンスガイド』の「ツール編」－「環境設定」－「ユーザー情報管理」、または「ツール編」－「ユーザー情報設定」－「ユーザー情報管理」をご覧ください。

認証デバイスのご購入時の設定は次のとおりです。

| 認証デバイス | 設定項目 | ご購入時の設定 |
|---|---|---|
| 指紋センサー | 指紋ユーザー名 | saadmin |
| 指紋センサー | バイオパスワード | administrator |
| IC カード（FeliCa 方式） | 利用者 PIN | 0000 |
| IC カード（FeliCa 方式） | 管理者 PIN | administrator 注 1 |
| スマートカード | 利用者 PIN | 0000 注 2 |
| スマートカード | 管理者 PIN | administrator 注 2 |
| セキュリティチップ | 所有者パスワード | administrator 注 3 |

注1:FMV オプション製品である FeliCa 対応非接触 IC カード（FMFLC-C1）を使用した場合の設定値です。それ以外のカードで作成や発行を行った場合はこの限りではありません。
注2:FMV オプション製品であるスマートカード（FMSMA-C1）を使用した場合の設定値です。それ以外のカードで作成や発行を行った場合はこの限りではありません。
注3:すでにセキュリティチップの所有者パスワードが設定されている場合、設定されている所有者パスワードが有効になります。

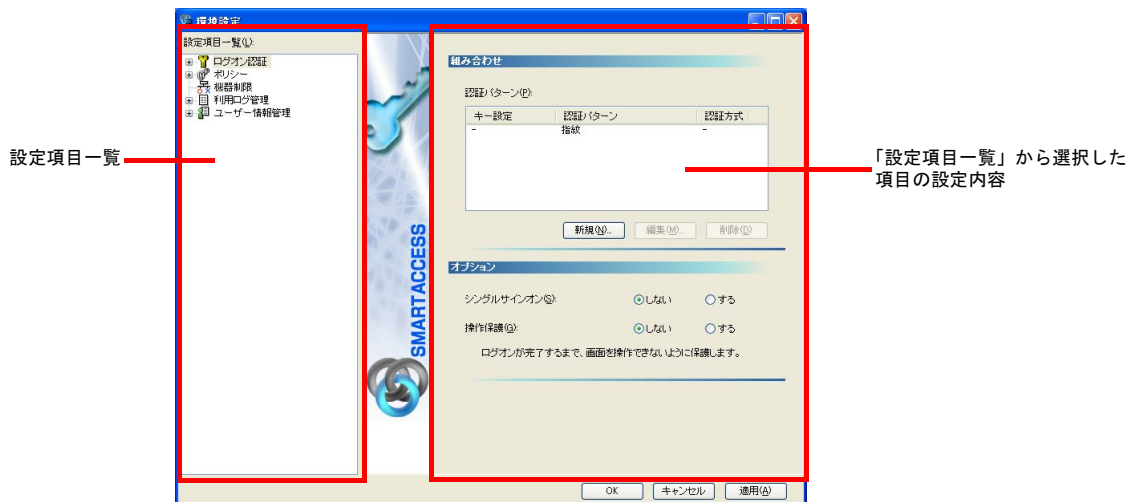
## 「環境設定」の起動

管理者が認証方法やセキュリティポリシーなどを設定するためのツール「環境設定」は、次の手順で起動します。

### 1 次の操作をします。

■ SMARTACCESS をインストールしたアカウントで Windows にログオンしている場合
「スタート」ボタン→「すべてのプログラム」→「SMARTACCESS」→「環境設定」の順にクリックします。

■ SMARTACCESS をインストールしたアカウント以外で Windows にログオンしている場合
SMARTACCESS をインストールしたフォルダ（→ P.23）にある「F5FZADMN.exe」を実行します。

「環境設定」が起動します。
左側の、機能をツリー構造で表示している領域を「設定項目一覧」と呼び、右側には「設定項目一覧」から選択した機能の設定内容を表示します。
「設定項目一覧」には、導入されてない認証デバイスや、インストールされていない連携ソフトウェアは表示されません。また、設定内容にはコンピュータ全体の設定が表示されます。

## 2 「設定項目一覧」から設定を行う項目をクリックして選択します。

## 3 選択した項目について設定を行います。

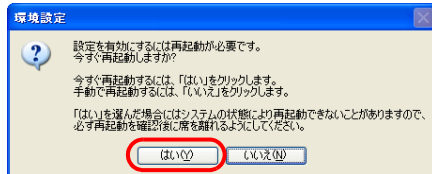
## 4 設定したら次の操作をします。

■ 続けて他の項目の設定をする場合

「適用」をクリックし、次に設定する項目をクリックして設定します。

■「環境設定」を終了する場合

「OK」をクリックします。

設定内容によっては Windows の再起動を要求するメッセージが表示されます。設定を有効にするために、「はい」をクリックして再起動してください。

# 2 指紋センサーをお使いの場合

ここでは、指紋センサーと SMARTACCESS を使って Windows へのログオン時の認証を行うための設定と、BIOS パスワードとの連携の設定について説明します。

## ■設定の流れ

### □管理者による設定

**1 認証パターンの登録の確認（→ P.36）**

**2 アカウントの登録（→ P.38）**

### □利用者による設定

**3 指紋の登録（→ P.42）**

### □管理者による設定

**4 Windows ログオンの設定（→ P.48）**

### □利用者による設定

**5 パスワードの変更（→ P.49）**

### □管理者による設定

**6 BIOS パスワードとの連携の設定（→ P.51）**

コンピュータ（BIOS）の起動時や BIOS セットアップの起動時にパスワードを入力する代わりに、指紋認証を使うことができます。また、シングルサインオン機能を使うことにより、コンピュータ（BIOS）の起動時の指紋認証のみで Windows にログオンすることもできます。
BIOS パスワードとの連携機能は BIOS パスワードとの連携機能に対応しているコンピュータでのみお使いになれます。

## ■ログオン手順

・指紋認証で Windows にログオンする（→ P.50）
・BIOS パスワードと指紋認証の連携（→ P.51）

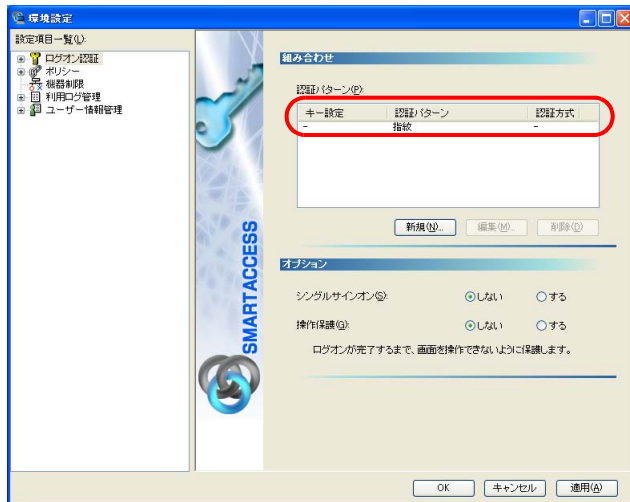
## 認証パターンの登録の確認

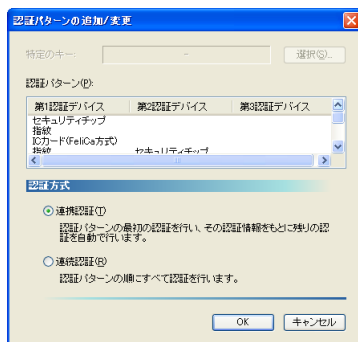
ログオン認証に使う認証デバイスと、複数の認証デバイスを使って認証する場合に設定する「認証方式」の組み合わせを認証パターンといいます。
認証パターンには、ドライバがインストールされている認証デバイスが自動的に登録され、一覧で表示されます。

**1 「環境設定」を起動します（→ P.34）。**

**2 「設定項目一覧」から「ログオン認証」をクリックします。**

「認証パターン」が表示されます。

## 3 「キー設定」の「－」の右隣に「指紋」が表示されていることを確認します。

「指紋」以外の認証パターンが表示されている場合には、次の手順で認証パターンを変更します。

1. 「キー設定」が「－」の認証パターンをクリックして選択し、「編集」をクリックします。
   「認証パターンの追加／変更」が起動します。

2. 「第 1 認証デバイス」が「指紋」、「第 2 認証デバイス」が空白の組合せをクリックして「OK」をクリックします。

複数の認証デバイスをお使いになる場合、「認証パターン」より認証デバイスと順序を選択してから「認証方式」を選択して登録します。詳しくは、『リファレンスガイド』の「機能編」－「ログオン認証」－「認証パターンの設定」をご覧ください。

**POINT**

- 「認証方式」には「連携認証」と「連続認証」があります。
  - ・連携認証
    1 つ目のデバイスで認証し、その認証情報をもとに以降の認証を自動で行う認証方式です。
    「第 1 認証デバイス」が「指紋」、「第 2 認証デバイス」が「セキュリティチップ」の認証パターンの場合、指紋認証を行うだけでユーザーキーパスワードを入力することなく認証できます。
  - ・連続認証
    認証パターンの順にすべての認証を行います。
    「第 1 認証デバイス」が「指紋」、「第 2 認証デバイス」が「セキュリティチップ」の認証パターンの場合、指紋認証を行った後にユーザーキーパスワードを入力する必要があります。
- 「特定のキー」とは
  認証時に「特定のキー」に設定したキーを押すことで、他の「認証パターン」に切り替えることができます。
  - ・Windows Vista の場合
    Windows ログオン時や「ユーザー情報設定」の起動時、【F9】キーに設定された「認証パターン」で認証ウィンドウが表示されます。
    そのときに「特定のキー」で設定したキーを押すと、認証ウィンドウをその「特定のキー」に設定した認証パターンに切り替えることができます。
  - ・Windows XP の場合
    Windows ログオン時に「Windows へようこそ」ウィンドウから認証ウィンドウに切り替えるとき、または「ユーザー情報設定」の起動時、【Ctrl】＋【Alt】＋【Delete】に設定された「認証パターン」で認証ウィンドウが表示されます。
    そのときに「特定のキー」で設定したキーを押すと、認証ウィンドウをその「特定のキー」に設定した認証パターンに切り替えることができます。

**4 続けてアカウントの登録を行う場合は、「適用」をクリックします。**

アカウントの登録を行う場合は、「アカウントの登録」(→ P.38)をご覧ください。

**POINT**

▶「環境設定」を終了するには、「OK」をクリックします。再起動を要求するメッセージが表示された場合は、Windows を再起動して設定を有効にします。

## アカウントの登録

SMARTACCESS を利用する管理者や利用者のアカウントは、「管理者ウィザード」で登録します。

**1 「環境設定」を起動します(→ P.34)。**

**2 「設定項目一覧」から「ユーザー情報管理」をクリックします。**

**3 「アカウント追加」の「起動」をクリックします。**

■ Windows Vista の場合

「ユーザーアカウント制御」ウィンドウが表示された場合は、開始されるプログラムを確認し、「続行」をクリックします。

「管理者ウィザード」ウィンドウが表示されます。

■ Windows XP の場合

「管理者ウィザード」ウィンドウが表示されます。

## 4 表示されている「認証の種類」と「認証デバイス」を確認し、「次へ」をクリックします。

「SMARTACCESS アカウントの登録」が表示されます。

## 5 SMARTACCESS で使用するアカウントを登録します。

複数の認証デバイスを使用する場合、「アカウント名」、「パスワード」は認証デバイスごとの制約をすべて満たすものを設定します。
他の認証デバイスの制約については、その認証デバイスの「アカウントの登録」のページをご覧ください。

- **アカウント名**
  個人を識別するアカウントを入力します。
  - 1 ～ 16 文字の半角英数字と記号 $()@_-.% で指定します。
  - 重複するユーザー名を使用することはできません。
- **パスワード**
  8 ～ 32 文字の半角英数字と記号 $()@_-.% で入力します。このパスワードがバイオパスワードとなります。
  「ポリシー」の「複雑さの設定」を設定している場合は、その設定内容に従って入力します。
  「複雑さの設定」については『リファレンスガイド』の「ツール編」－「環境設定」－「ポリシー」－「指紋」をご覧ください。
- **パスワードの確認入力**
  確認として「パスワード」で入力したものと同じ内容を入力します。

## 6 「次へ」をクリックします。

「Windows ユーザーの登録」が表示されます。

## 7 Windows ユーザーを登録します。

・Windows ユーザー名
「Windows ユーザー名」の右の▼をクリックして Windows アカウントを選択します。
ドメインに参加している場合、「ドメイン」を選択してから「Windows ユーザー名」の右の▼をクリックするとそのドメイン内の Windows アカウントを選択できます。
「Windows ユーザー名」に「ドメイン ¥Windows ユーザー名」とは入力しないでください。Windows ユーザー名とドメイン名は、それぞれの項目に分けて入力してください。

・ドメイン
ドメインに参加している場合は、「ドメイン」の▼をクリックしてドメインを選択します。

・パスワード
「Windows ユーザー名」で選択した Windows アカウントに登録されているパスワードを入力します。

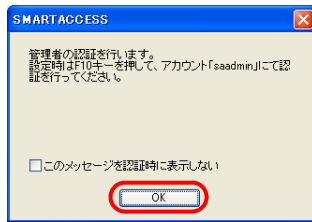
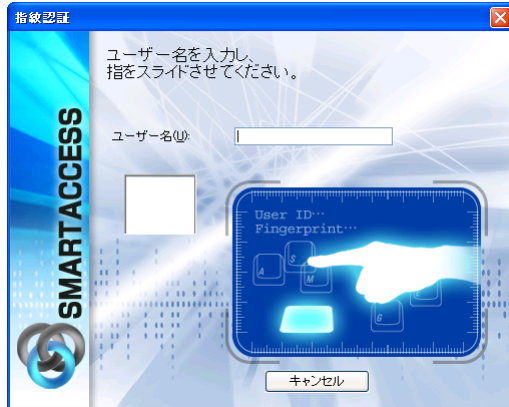
・パスワード入力確認
確認として「パスワード」と同じ内容を入力します。

## 8 「次へ」をクリックします。

「設定の確認」が表示されます。

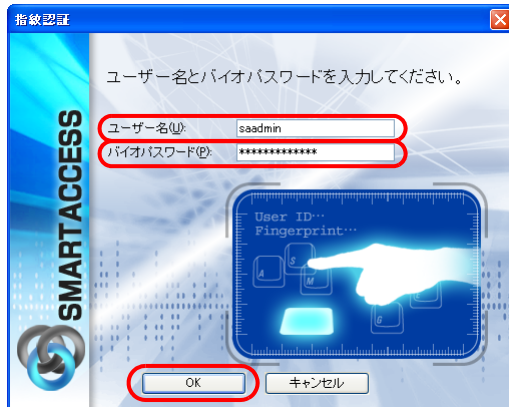
## 9 「設定内容」を確認し、「次へ」をクリックします。

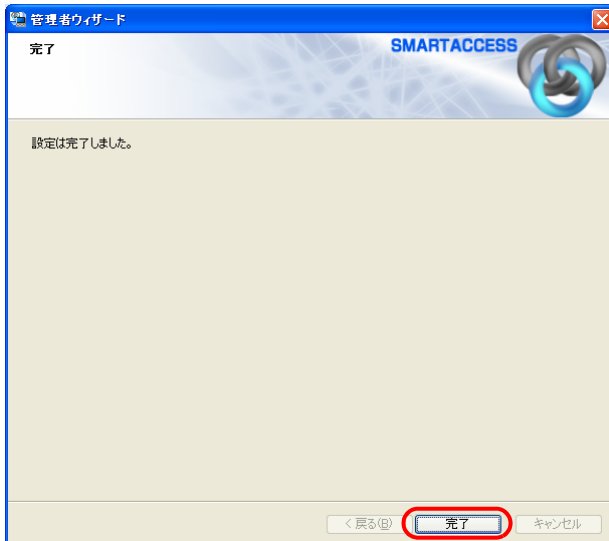
管理者の認証を要求するウィンドウが表示されます。

## 10 「OK」をクリックします。

「指紋認証」ウィンドウが表示されます。

## 11 まだ指紋の登録を行っていないので、バイオパスワード認証に切り替えるために【F10】キーを押します。

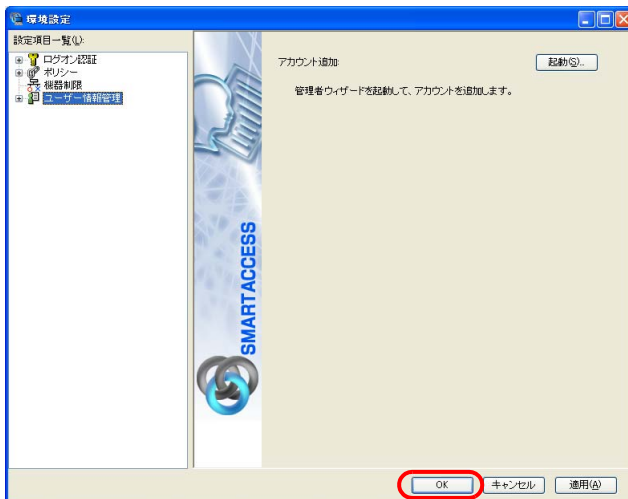
「ユーザー名とバイオパスワードを入力してください。」と表示されます。

## 12 「ユーザー名」と「バイオパスワード」を入力し、「OK」をクリックします。

「ユーザー名」に「saadmin」、「バイオパスワード」に「administrator」と入力し、「OK」をクリックします。

「完了」と表示されます。

## 13 「完了」をクリックします。

「環境設定」に戻ります。

## 14 「OK」をクリックして「環境設定」を終了します。

再起動を要求するメッセージが表示された場合は、Windows を再起動してください。

# 指紋の登録

指紋センサーをお使いになるには、認証用の指紋の登録が必要です。
指にけがをしたときなどのために必ず 2 本の指の指紋を登録してください。

## 1 コンピュータを起動します。

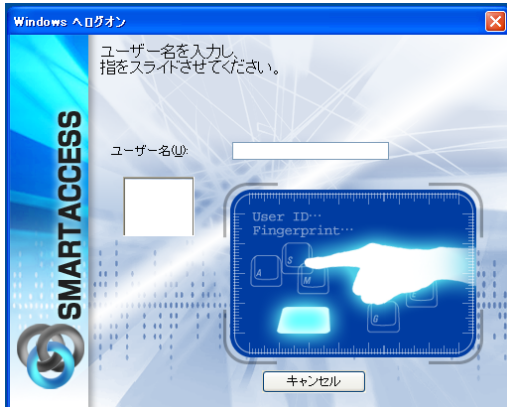
■ Windows Vista をお使いの場合

「Windows へログオン」ウィンドウが表示されます。
手順 3 に進んでください。

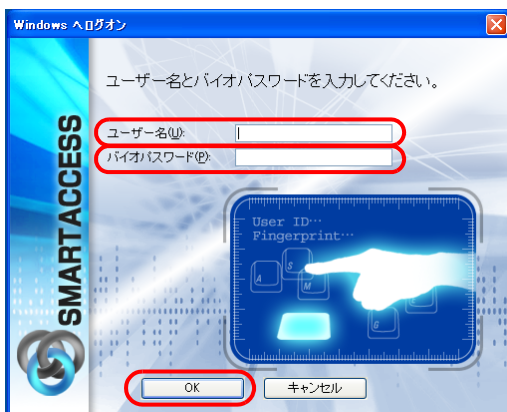
■ Windows XP をお使いの場合

「Windows へようこそ」ウィンドウが表示されます。

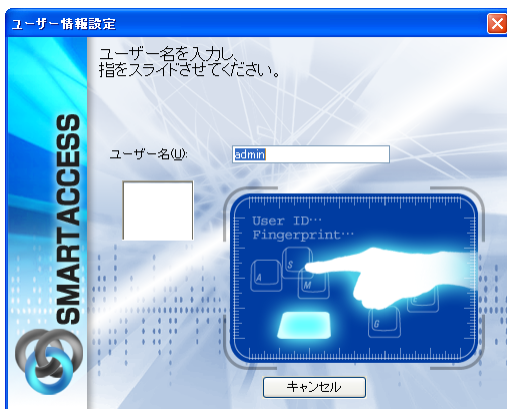
## 2 【Ctrl】＋【Alt】＋【Delete】キーを押します。

「Windows へログオン」ウィンドウの認証画面が表示されます。

## 3 まだ指紋の登録を行っていないので、【F10】キーを押して、バイオパスワード認証ウィンドウに切り換えます。

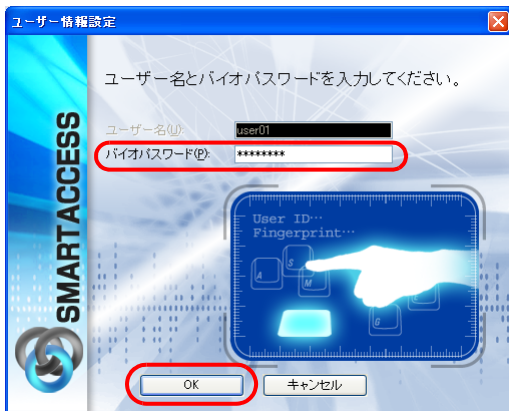
「Windows へログオン」ウィンドウの「ユーザー名とバイオパスワードを入力する」が表示されます。

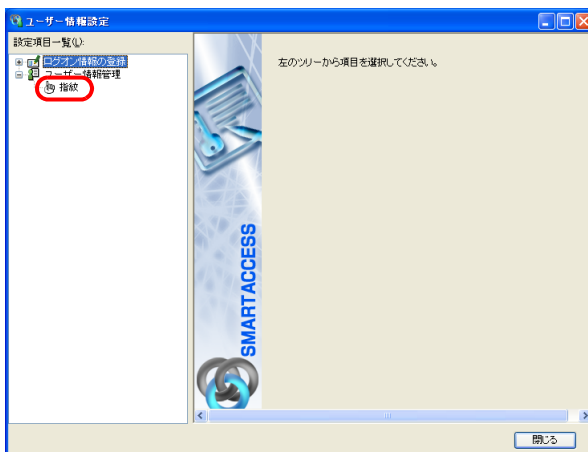
## 4 指紋を登録する利用者アカウントの「ユーザー名」「バイオパスワード」を入力して、「OK」をクリックします。

Windows が起動します。

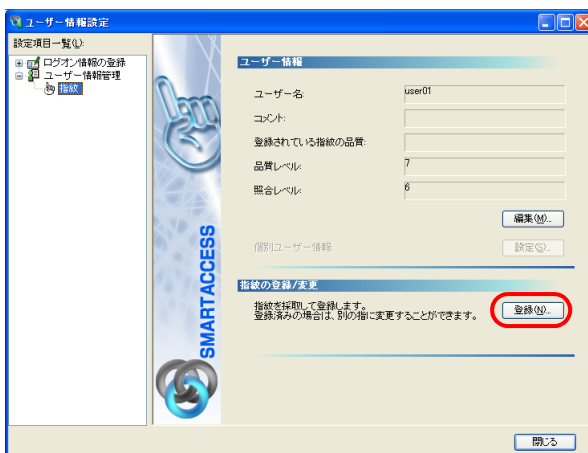
## 5 「スタート」ボタン→「すべてのプログラム」→「SMARTACCESS」→「ユーザー情報設定」の順にクリックします。

「ユーザー情報設定」ウィンドウの認証画面が表示されます。

## 6 まだ指紋の登録を行っていないので、【F10】キーを押して、バイオパスワード認証ウィンドウに切り換えます。

「ユーザー情報設定」ウィンドウの「ユーザー名とバイオパスワードを入力する」が表示されます。

## 7 指紋を登録する利用者アカウントの「バイオパスワード」を入力して、「OK」をクリックします。

「ユーザー情報設定」ウィンドウが表示されます。

## 8 「設定項目一覧」から「ユーザー情報管理」→「指紋」の順にクリックします。

起動時に認証したアカウントの指紋情報が表示されます。

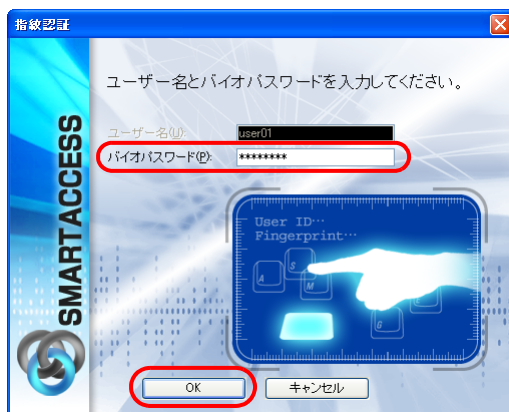
## 9 内容を確認して、「登録」をクリックします。

「ユーザー名を入力し、指をスライドさせてください。」が表示されます。

**POINT**

- 指紋登録のとき、【F10】キーを押さずに手順 10 のバイオパスワード認証ウィンドウが最初に表示されるように設定を変更することができます。
  「環境設定」の「ポリシー」→「指紋」にある「認証モード」で「指紋登録時にバイオパスワード認証を使用」を「する」と設定します。詳しくは『リファレンスガイド』の「ツール編」－「環境設定」－「ポリシー」－「指紋」をご覧ください。

## 10 【F10】キーを押して、バイオパスワード認証ウィンドウに切り換えます。

「ユーザー名とバイオパスワードを入力してください。」が表示されます。

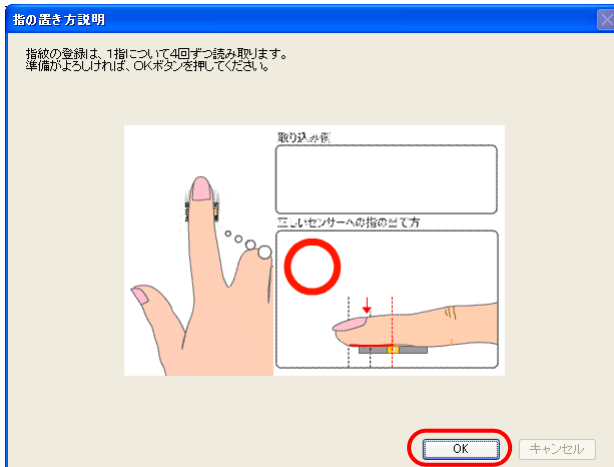
## 11 指紋を登録する利用者アカウントの「バイオパスワード」を入力して、「OK」をクリックします。

「指紋の登録／変更」ウィンドウが表示されます。

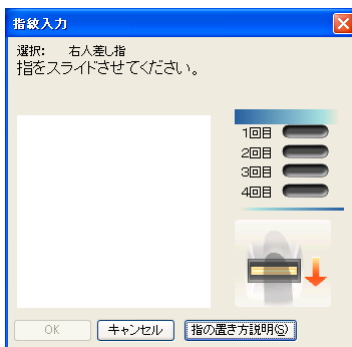
## 12 指紋を登録する指をクリックして、「登録／変更」をクリックします。

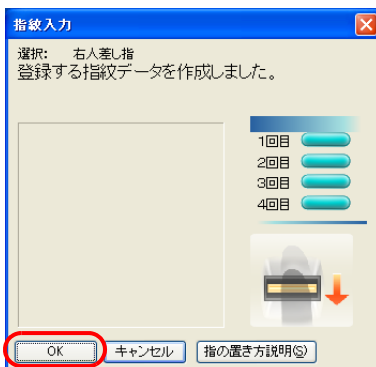
**POINT**

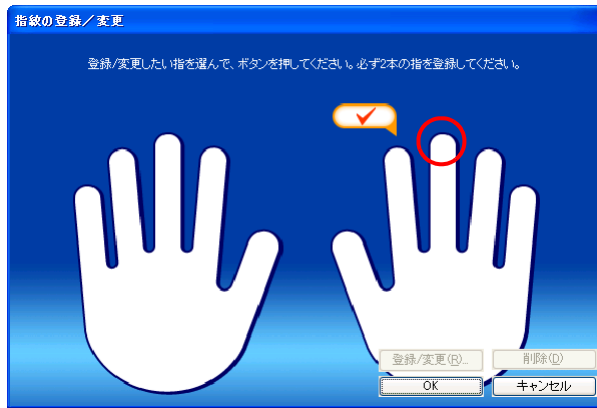
- 間違えて別の指をクリックした場合は、「キャンセル」をクリックして再度「登録／変更」をクリックし直します。

「指の置き方説明」ウィンドウが表示されます。

## 13 内容を確認して、「OK」をクリックします。

「指紋入力」ウィンドウが表示されます。

## 14 表示されるメッセージに従って、指紋の読み取りを 4 回行います。

指紋の読み取り方については「認証デバイスの取り扱い」—「指紋センサー」—「指紋の読み取り方」(→ P.88)をご覧ください。
4 回の読み取りが正しく完了すると「登録する指紋データを作成しました。」と表示されます。

## 15 「OK」をクリックします。

「指紋の登録／変更」ウィンドウが表示されます。

**16** **2 本目に登録する指をクリックし、手順 14 〜 15 の操作を行います。**

「指紋の登録 / 変更」ウィンドウが表示されます。

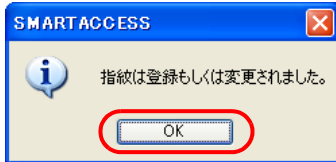
**17** **登録した指にチェックマークが設定されていることを確認し、「OK」をクリックして、指紋情報を登録します。**

**POINT**

- 登録した指紋を取り消すには、登録した指をクリックして「削除」をクリックします。

- 「キャンセル」をクリックすると指紋の登録を中断して「ユーザー情報設定」ウィンドウに戻ります。

「指紋は登録もしくは変更されました。」と表示されます。

**18** **「OK」をクリックします。**

「ユーザー情報設定」ウィンドウに戻ります。

**19** **「閉じる」をクリックして「ユーザー情報設定」を終了します。**

**20** **「ユーザー情報設定」を起動し認証画面で指紋認証を行い、指紋を登録できたことを確認します。**

認証に成功すれば登録成功です。

## Windows ログオンの設定

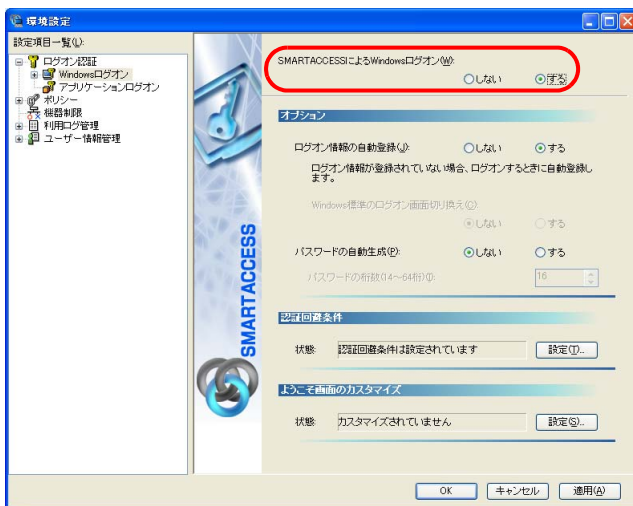
ここでは、Windows のログオン認証を、従来の Windows パスワードの認証から SMARTACCESS を使った認証に変更する手順を説明します。
Windows ログオンに関連する他の機能については『リファレンスガイド』の「機能編」－「ログオン認証」－「Windows ログオン」をご覧ください。

### ■Windows ログオンを有効にする

Windows ログオンを利用するには、「SMARTACCESS による Windows ログオン」を有効にします。

**1** **「環境設定」を起動します（→ P.34）。**

**2** **「設定項目一覧」から「ログオン認証」→「Windows ログオン」の順にクリックします。**

**3** **「SMARTACCESS による Windows ログオン」の「する」をクリックします。**

**4** **「OK」をクリックして「環境設定」を終了します。**

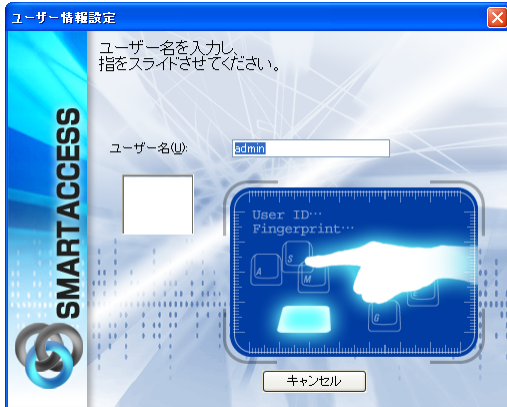
再起動を要求するメッセージが表示された場合は、Windows を再起動して設定を有効にします。

# パスワードの変更

## ■バイオパスワードを変更する

利用者がバイオパスワードの変更をすることで、バイオパスワードを知っているのは利用者本人だけになります。セキュリティを強化するためにも、SMARTACCESS運用開始時に利用者自身でバイオパスワードを変更することをお勧めします。

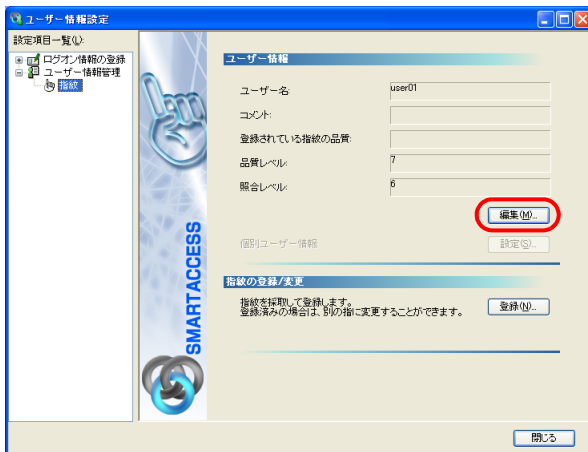
**1** **「スタート」ボタン→「すべてのプログラム」→「SMARTACCESS」→「ユーザー情報設定」の順にクリックします。**

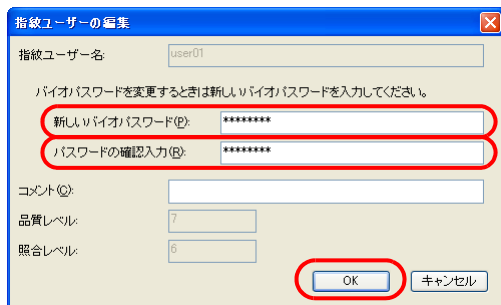
「ユーザー情報設定」ウィンドウの認証画面が表示されます。

**2** **ウィンドウのメッセージに従って指紋の読み取りを行います。**

認証されると「ユーザー情報設定」が起動します。

**3** **「設定項目一覧」から「ユーザー情報管理」→「指紋」の順にクリックします。**

起動時に認証したアカウントの指紋情報が表示されます。

**4** **「ユーザー情報」の「編集」をクリックします。**

「指紋ユーザーの編集」ウィンドウが表示されます。

**5** **「新しいバイオパスワード」「パスワードの確認入力」を入力し、「OK」をクリックします。**

・**新しいバイオパスワード**
変更後のバイオパスワードを、8 ～ 32 文字の半角英数字と記号 $()@_-.% で入力します。
「ポリシー」で複雑さの設定を行っている場合はその設定に従って入力します。
「複雑さの設定」については『リファレンスガイド』の「ツール編」－「環境設定」－「ポリシー」－「指紋」をご覧ください。

・**パスワードの確認入力**
確認として「新しいバイオパスワード」と同じ内容を入力します。

「ユーザー情報設定」ウィンドウに戻ります。

**6** **「閉じる」をクリックして、「ユーザー情報設定」を終了します。**

## 指紋認証で Windows にログオンする

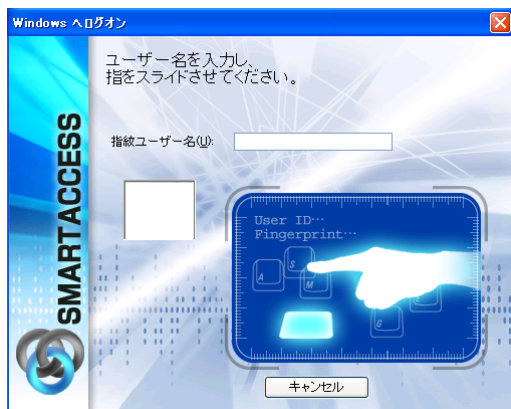
ここでは、指紋センサーを利用して Windows ログオンをする手順を説明します。

**1** **コンピュータを起動します。**

■ Windows Vista をお使いの場合
「Windows へログオン」ウィンドウが表示されます。
手順 3 に進んでください。

■ Windows XP をお使いの場合
「Windows へようこそ」ウィンドウが表示されます。

**2** **【Ctrl】＋【Alt】＋【Delete】キーを押します。**

「Windows へログオン」ウィンドウの認証画面が表示されます。

**3** **「ユーザー名」に「SMARTACCESS アカウント」を入力し、指紋の読み取りを行います。**

認証が行われ、Windows にログオンします。

# BIOS パスワードと指紋認証の連携

コンピュータ（BIOS）の起動時や BIOS セットアップの起動時にパスワードを入力する代わりに、指紋認証を使うことができます。
ここでは、「Windows ログオンとのシングルサインオン」、「BIOS 指紋ユーザーの新規登録」、および「BIOS パスワードの有効化」の設定について説明します。
BIOS パスワードとの連携機能は、この機能に対応しているコンピュータでのみお使いになれます。

**1 コンピュータを起動します。**

指紋認証画面が表示されます。

**2 認証タイプで「指紋認証」を選択し、指紋の読み取りを行います。**

認証が行われるとコンピュータが起動します。

■ Windows Vista をお使いの場合

しばらくすると Windows にログオンします。

■ Windows XP をお使いの場合

「Windows へようこそ」ウィンドウが表示されます。

1.【Ctrl】+【Alt】+【Delete】キーを押します。

Windows にログオンします。

設定の流れは次のとおりです。

**1 BIOS シングルサインオンを有効にする（→ P.51）**

**2 BIOS 指紋ユーザーの登録（→ P.52）**

**3 BIOS パスワードを有効にする（→ P.53）**

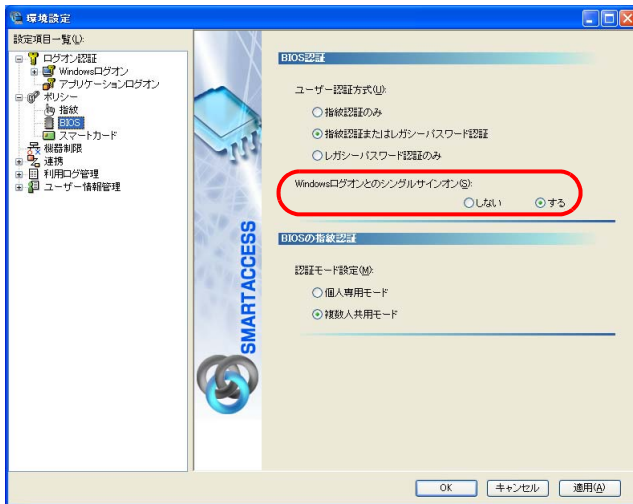
## ■BIOS シングルサインオンを有効にする

この設定をすると、コンピュータ（BIOS）の起動時に指紋認証を行えばもう一度指紋認証をしないで Windows にログオンすることができます。

**1 「環境設定」を起動します（→ P.34）。**

**2 「設定項目一覧」から「ポリシー」→「BIOS」をクリックします。**

「BIOS 認証」の詳細が表示されます。

### 3 「Windows ログオンとのシングルサインオン」の「する」をクリックします。

- ご購入時の「ユーザー認証方式」は「指紋認証またはレガシーパスワード認証」となっています。
  「ユーザー認証方式」が「指紋認証のみ」の場合、登録した指紋の品質が悪い場合や指にけがをしたときに、コンピュータにログオンできなくなることがありますのでご注意ください。
- 指紋で認証して BIOS セットアップを起動すると、BIOS セットアップの「管理者」ではなく「ユーザー」となります。BIOS セットアップの「管理者」として認証するためには、指紋ではなくパスワードによる認証を行う必要があります。
  「ユーザー認証方式」を「指紋認証のみ」に設定している場合に、管理者として BIOS セットアップを起動するためには、いったん「ユーザー認証方式」を「指紋認証またはレガシーパスワード認証」に変更して再起動し、BIOS セットアップでの認証はパスワードで行ってください。

詳しくは、『リファレンスガイド』の「ツール編」－「環境設定」－「ポリシー」－「BIOS」をご覧ください。

## ■BIOS 指紋ユーザーの登録

BIOS に指紋を登録する前に、あらかじめ指紋を登録する SMARTACCESS アカウントを登録したうえで、指紋を登録しておく必要があります。指紋を登録していない SMARTACCESS アカウントを BIOS に登録することはできません。登録人数は 10 人までです。

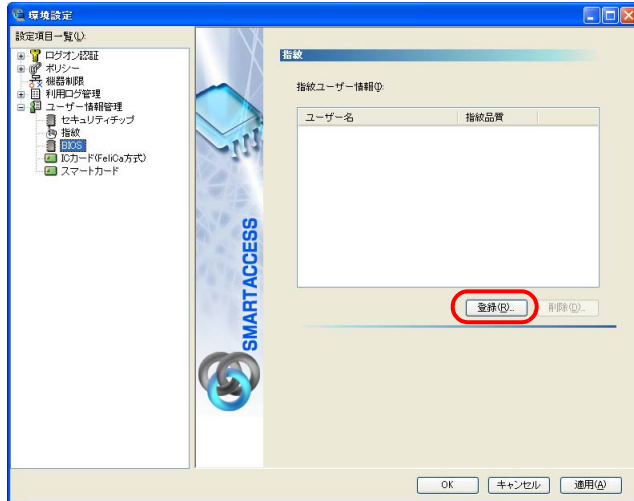
### 1 「環境設定」を起動します（→ P.34）。

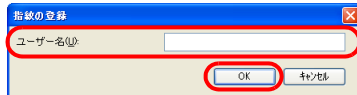
### 2 「ユーザー情報管理」→「BIOS」の順にクリックします。

指紋認証画面が表示されます。

### 3 指紋を入力して認証を行います。

「指紋ユーザー情報」が表示されます。

### 4 「指紋ユーザー情報」の「登録」をクリックします。

「指紋の登録」ウィンドウが表示されます。

### 5 「ユーザー名」に BIOS 指紋認証を行う SMARTACCESS アカウントを入力し、「OK」をクリックします。

ユーザー名は大文字小文字を区別します。BIOS に登録するときに入力するユーザー名は、指紋ユーザー名と一致するように入力してください。

### 6 登録の確認後、「環境設定」で「OK」をクリックします。

## ■BIOS パスワードを設定する

コンピュータを再起動し、BIOS セットアップで「起動時のパスワード」を設定し、BIOS セットアップの起動時にパスワードの認証が必要となるようにします。
BIOS セットアップの起動と設定は、お使いのコンピュータによって異なります。詳しくは、コンピュータ本体の『製品ガイド』の「BIOS」をご覧ください。

## ■BIOS の「指紋ユーザー情報」の削除

指紋と BIOS パスワードとの連携機能では、指紋の情報を BIOS 内に格納しています。
BIOS 内に格納されている指紋の情報を削除する場合は「ユーザー情報管理」→「BIOS」から、指紋ユーザー情報を削除する必要があります。
詳しくは、『リファレンスガイド』の「ツール編」－「環境設定」－「ユーザー情報管理」－「BIOS」をご覧ください。

# 3 FeliCa 対応リーダ／ライタをお使いの場合

ここでは、FeliCa 対応リーダ／ライタと SMARTACCESS を使って Windows へのログオン時の認証を行うための設定と、カード操作によるコンピュータのロックを行うための設定について説明します。

## ■設定の流れ

### □管理者による設定

1 **認証パターンの登録の確認（→ P.54）**

2 **アカウントの登録（→ P.56）**

3 **Windows ログオンの設定（→ P.60）**

4 **カード操作によるコンピュータのロックを行うための設定（→ P.60）**

### □利用者による設定

5 **パスワードの変更（→ P.61）**

## ■ログオン手順

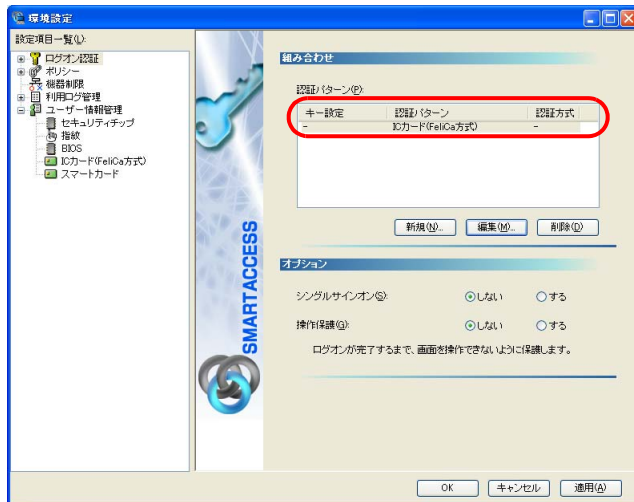
・IC カード（FeliCa 方式）認証で Windows にログオンする（→ P.63）

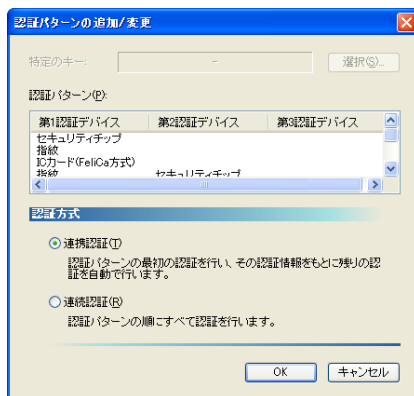
## 認証パターンの登録の確認

ログオン認証に使う認証デバイスと、複数の認証デバイスを使って認証する場合に設定する「認証方式」の組み合わせを認証パターンといいます。
認証パターンには、ドライバがインストールされている認証デバイスが自動的に登録され、一覧で表示されます。

1 **「環境設定」を起動します（→ P.34）。**

2 **「設定項目一覧」から「ログオン認証」をクリックします。**
「認証パターン」が表示されます。

## 3 「キー設定」の「−」の右隣に「IC カード（FeliCa 方式）」が表示されていることを確認します。

「IC カード（FeliCa 方式）」以外の認証パターンが表示されている場合には、次の手順で認証パターンを変更します。

1. 「キー設定」が「−」の認証パターンをクリックして選択し、「編集」をクリックします。
   「認証パターンの追加／変更」が起動します。

2. 「第 1 認証デバイス」が「IC カード（FeliCa 方式）」、「第 2 認証デバイス」が空白の組合せをクリックして「OK」をクリックします。

複数の認証デバイスをお使いになる場合、「認証パターン」より認証デバイスと順序を選択してから「認証方式」を選択して登録します。詳しくは、『リファレンスガイド』の「機能編」−「ログオン認証」−「認証パターンの設定」をご覧ください。

### POINT

▶「認証方式」には「連携認証」と「連続認証」があります。
- 連携認証
  1 つ目のデバイスで認証し、その認証情報をもとに以降の認証を自動で行う認証方式です。
  「第 1 認証デバイス」が「IC カード（FeliCa 方式）」、「第 2 認証デバイス」が「セキュリティチップ」の認証パターンの場合、IC カード（FeliCa 方式）で認証を行うだけでユーザーキーパスワードを入力することなく認証できます。
- 連続認証
  認証パターンの順にすべての認証を行います。
  「第 1 認証デバイス」が「IC カード（FeliCa 方式）」、「第 2 認証デバイス」が「セキュリティチップ」の認証パターンの場合、IC カード（FeliCa 方式）で認証を行った後にユーザーキーパスワードを入力する必要があります。

▶「特定のキー」とは
認証時に「特定のキー」に設定したキーを押すことで、他の「認証パターン」に切り替えることができます。
- Windows Vista の場合
  Windows ログオン時や「ユーザー情報設定」の起動時、【F9】キーに設定された「認証パターン」で認証ウィンドウが表示されます。
  そのときに「特定のキー」で設定したキーを押すと、認証ウィンドウをその「特定のキー」に設定した認証パターンに切り替えることができます。

・Windows XP の場合
Windows ログオン時に「Windows へようこそ」ウィンドウから認証ウィンドウに切り替えるとき、または「ユーザー情報設定」の起動時、【Ctrl】+【Alt】+【Delete】に設定された「認証パターン」で認証ウィンドウが表示されます。
そのときに「特定のキー」で設定したキーを押すと、認証ウィンドウをその「特定のキー」に設定した認証パターンに切り替えることができます。

**4 続けてアカウントの登録を行う場合は、「適用」をクリックします。**

アカウントの登録を行う場合は、「アカウントの登録」（→ P.56）をご覧ください。

**POINT**

- 「環境設定」を終了するには、「OK」をクリックします。再起動を要求するメッセージが表示された場合は、Windows を再起動して設定を有効にします。

## アカウントの登録

SMARTACCESS を利用する管理者や利用者のアカウントは、「管理者ウィザード」で登録します。

**1 「環境設定」を起動します（→ P.34）。**

**2 「設定項目一覧」から「ユーザー情報管理」をクリックします。**

**3 「アカウント追加」の「起動」をクリックします。**

■ Windows Vista の場合
「ユーザーアカウント制御」ウィンドウが表示された場合は、開始されるプログラムを確認し、「続行」をクリックします。
「管理者ウィザード」ウィンドウが表示されます。

■ Windows XP の場合
「管理者ウィザード」ウィンドウが表示されます。

## 4 表示されている「認証の種類」と「認証デバイス」を確認し、「次へ」をクリックします。

「SMARTACCESS アカウントの登録」が表示されます。

## 5 SMARTACCESS で使用するアカウントを登録します。

複数の認証デバイスを使用する場合、「アカウント名」、「パスワード」は認証デバイスごとの制約をすべて満たすものを設定します。
他の認証デバイスの制約については、その認証デバイスの「アカウントの登録」のページをご覧ください。

**・アカウント名**

個人を識別するアカウントを入力します。

- 文字数や使用文字の制限はありません。
- 重複するユーザー名を使用することができます。

**・パスワード**

1 〜 16 文字の半角英数字と記号で入力します。このパスワードが PIN となります。
「ポリシー」の「複雑さの設定」を設定している場合は、その設定内容に従って入力します。
「複雑さの設定」については『リファレンスガイド』の「ツール編」－「環境設定」－「ポリシー」－「IC カード（FeliCa 方式）」をご覧ください。

**・パスワードの確認入力**

確認として「パスワード」で入力したものと同じ内容を入力します。

## 6 「次へ」をクリックします。

「Windows ユーザーの登録」が表示されます。

## 7 Windows ユーザーを登録します。

・Windows ユーザー名

「Windows ユーザー名」の右の▼をクリックして Windows アカウントを選択します。
ドメインに参加している場合、「ドメイン」を選択してから「Windows ユーザー名」の右の▼をクリックするとそのドメイン内の Windows アカウントを選択できます。
「Windows ユーザー名」に「ドメイン ¥Windows ユーザー名」とは入力しないでください。Windows ユーザー名とドメイン名は、それぞれの項目に分けて入力してください。

・ドメイン

ドメインに参加している場合は、「ドメイン」の▼をクリックしてドメインを選択します。

・パスワード

「Windows ユーザー名」で選択した Windows アカウントに登録されているパスワードを入力します。

・パスワード入力確認

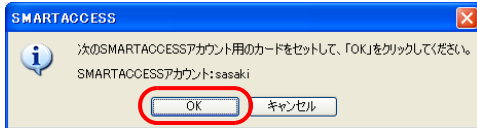
確認として「パスワード」と同じ内容を入力します。

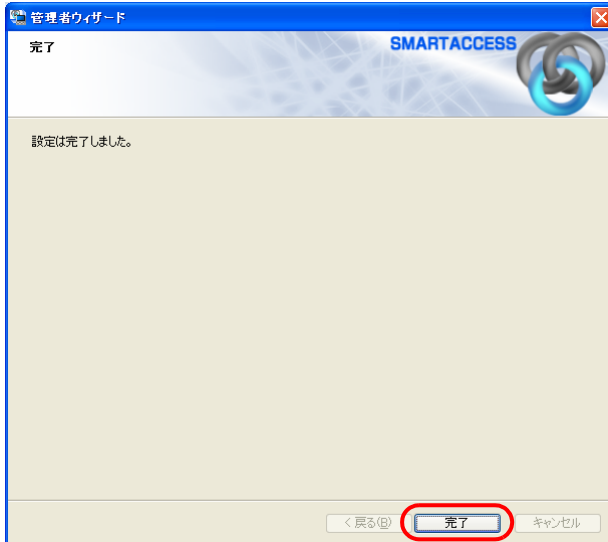
## 8 「次へ」をクリックします。

「設定の確認」が表示されます。

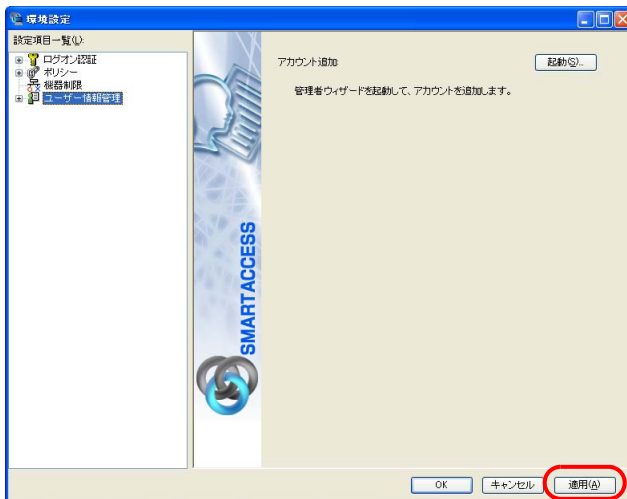
## 9 「設定内容」を確認し、「次へ」をクリックします。

カードのセットを要求するウィンドウが表示されます。

## 10 リーダ／ライタにカードをセットし、「OK」をクリックします。

「完了」と表示されます。

## 11 「完了」をクリックします。

「環境設定」に戻ります。

## 12 続けて Windows ログオンの設定を行う場合は、「適用」をクリックします。

Windows ログオンの設定を行う場合は、「Windows ログオンの設定」（→ P.60）をご覧ください。

**POINT**

- 「環境設定」を終了するには、「OK」をクリックします。再起動を要求するメッセージが表示された場合は、Windows を再起動して設定を有効にします。

# Windows ログオンの設定

ここでは、Windows のログオン認証を、従来の Windows パスワードの認証から SMARTACCESS を使った認証に変更する手順を説明します。
Windows ログオンに関連する他の機能については『リファレンスガイド』の「機能編」－「ログオン認証」－「Windows ログオン」をご覧ください。

## ■Windows ログオンを有効にする

Windows ログオンを利用するには、「SMARTACCESS による Windows ログオン」を有効にします。

1 「環境設定」を起動します（→ P.34）。

2 「設定項目一覧」から「ログオン認証」→「Windows ログオン」の順にクリックします。

3 「SMARTACCESS による Windows ログオン」の「する」をクリックします。

4 「OK」をクリックして「環境設定」を終了します。
再起動を要求するメッセージが表示された場合は、Windows を再起動して設定を有効にします。

# カード操作によるコンピュータのロック

詳しくは『リファレンスガイド』の「機能編」－「ログオン認証」－「カードのポーリング動作」をご覧ください。

## ■「カードのポーリング動作」の設定をする

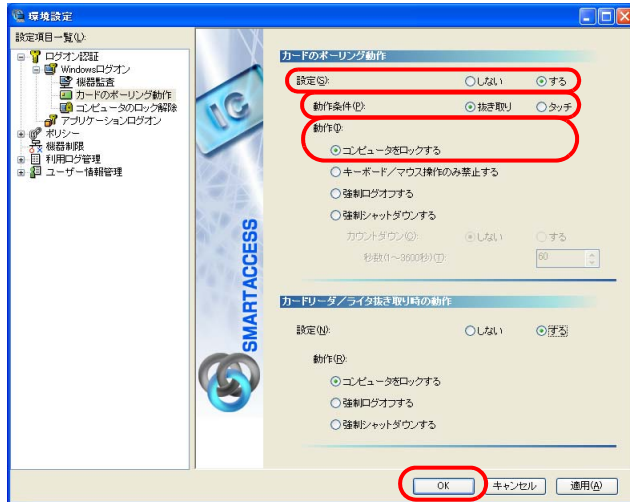
**重要**

- あらかじめ認証パターンに「IC カード（FeliCa 方式）」を含む組み合わせを設定し、「SMARTACCESS による Windows ログオン」を「する」に設定してください。

1 「環境設定」を起動します（→ P.34）。

2 「設定項目一覧」から「ログオン認証」→「Windows ログオン」→「カードのポーリング動作」をクリックします。
「カードのポーリング動作」の詳細が表示されます。

### 3 次の項目を設定し、「OK」をクリックします。

・「カードのポーリング動作」－「設定」
「する」をクリックします。
・「動作条件」
「抜き取り」をクリックします。
・「動作」
「コンピュータをロックする」をクリックします。

**重要**

▶「カードのポーリング動作」を「強制ログオフする」または「強制シャットダウンする」に設定している場合は、Windows のアクティブデスクトップ機能を利用しないでください。

## ■コンピュータのロックと解除

カードのポーリング動作を設定すると、カードを利用して Windows ログオンした後は、カードをリーダ／ライタから外したり、カードをリーダ／ライタにタッチしたりするだけでコンピュータをロックすることができます。
コンピュータのロックを解除する場合は、次の操作を行います。

### □Windows Vista をお使いの場合

カードをセットして PIN を入力します。

### □Windows XP をお使いの場合

【Ctrl】+【Alt】+【Delete】キーを押します。認証画面が表示されるので、カードをセットして PIN を入力します。

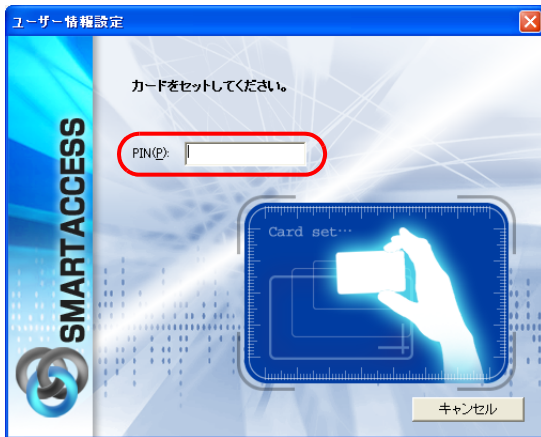
# パスワードの変更

## ■PIN を変更する

利用者が PIN の変更をすることで、PIN を知っているのは利用者本人だけになります。セキュリティを強化するためにも、SMARTACCESS 運用開始時に利用者自身で PIN を変更することをお勧めします。

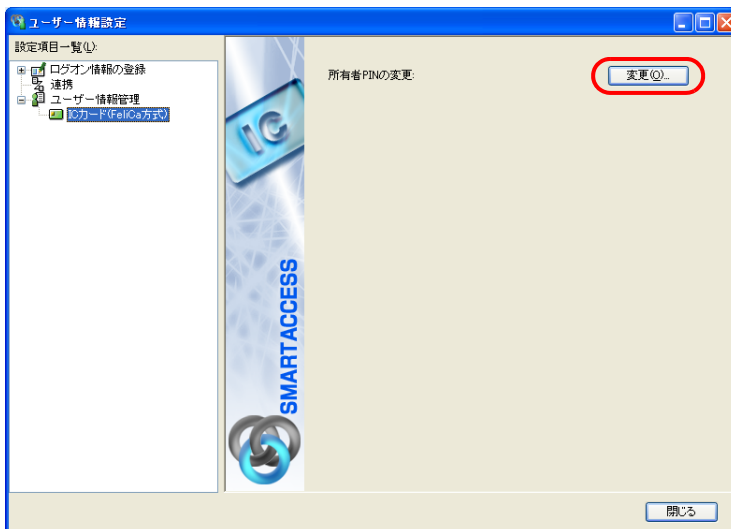
### 1 「スタート」ボタン→「すべてのプログラム」→「SMARTACCESS」→「ユーザー情報設定」の順にクリックします。

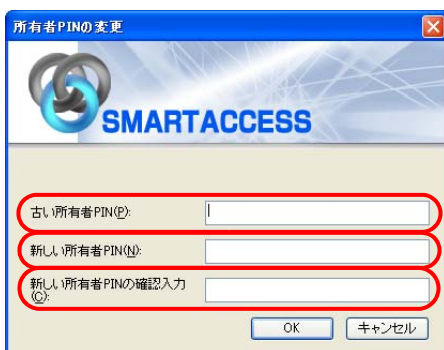
「ユーザー情報設定」ウィンドウの認証画面が表示されます。

## 2 リーダ／ライタにカードをセットし、PIN を入力します。

認証されると「ユーザー情報設定」が起動します。

## 3 「設定項目一覧」から「ユーザー情報管理」→「IC カード（FeliCa 方式）」の順にクリックします。

IC カード（FeliCa 方式）のユーザー設定画面が表示されます。

## 4 「変更」をクリックします。

「所有者 PIN の変更」ウィンドウが表示されます。

## 5 「古い所有者 PIN」、「新しい所有者 PIN」および「新しい所有者 PIN の確認入力」を入力します。

・古い所有者 PIN

現在 IC カード（FeliCa 方式）に登録されている所有者 PIN を入力します。

・新しい所有者 PIN
変更後の所有者 PIN を、1 ～ 16 文字の半角英数字と記号で入力します。
「ポリシー」で複雑さの設定を行っている場合はその設定に従って入力します。
「複雑さの設定」については『リファレンスガイド』の「ツール編」－「環境設定」－「ポリシー」－「IC カード（FeliCa 方式）」をご覧ください。
・新しい所有者 PIN の確認入力
確認として「新しい所有者 PIN」と同じ内容を入力します。

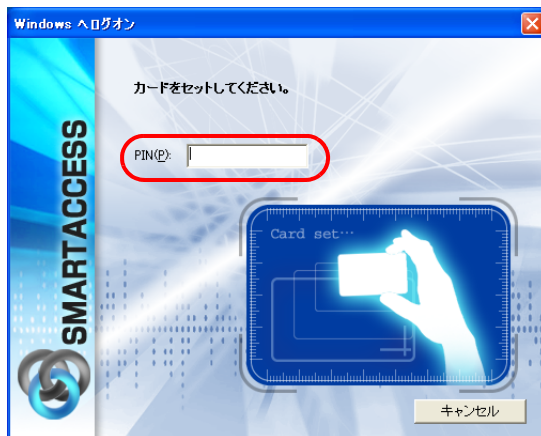
**6** **「OK」をクリックします。**
「ユーザー情報設定」ウィンドウに戻ります。

**7** **「閉じる」をクリックして、「ユーザー情報設定」を終了します。**

## IC カード（FeliCa 方式）で Windows にログオンする

**1** **コンピュータを起動します。**
■ Windows Vista をお使いの場合
「Windows へログオン」ウィンドウが表示されます。
手順 3 に進んでください。
■ Windows XP をお使いの場合
「Windows へようこそ」ウィンドウが表示されます。

**2** **【Ctrl】＋【Alt】＋【Delete】キーを押します。**
「Windows へログオン」ウィンドウが表示されます。

**3** **リーダ／ライタにカードをセットし、PIN を入力します。**

認証が行われ、Windows にログオンします。

# 4 スマートカードリーダ／ライタ、スマートカードホルダーをお使いの場合

ここでは、スマートカードと SMARTACCESS を使って Windows へのログオン時の認証を行うための設定、カード操作によるコンピュータのロックを行うための設定、および BIOS パスワードとの連携の設定について説明します。

### ■設定の流れ

**□管理者による設定**

1. **認証パターンの登録の確認（→ P.64）**
2. **アカウントの登録（→ P.66）**
3. **Windows ログオンの設定（→ P.70）**
4. **カード操作によるコンピュータのロックを行うための設定（→ P.71）**

**□利用者による設定**

5. **パスワードの変更（→ P.72）**

**□管理者による設定**

6. **BIOS パスワードとの連携の設定（→ P.74）**
   BIOS パスワードとの連携機能を利用すると、コンピュータ（BIOS）の起動時にスマートカードを使って認証することができます。
   この機能は BIOS パスワードとの連携機能に対応しているコンピュータでのみお使いになれます。

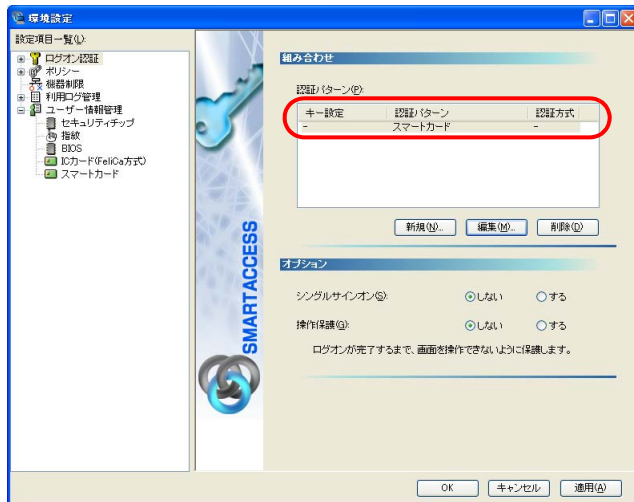
### ■ログオン手順

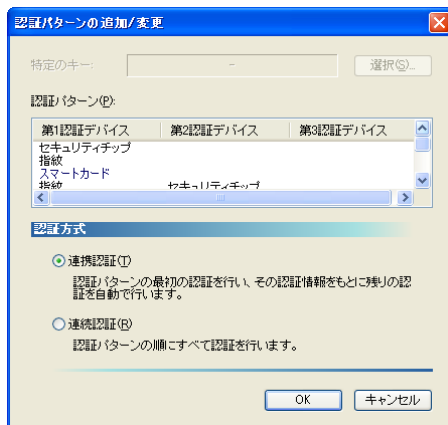
・スマートカード認証で Windows にログオンする（→ P.73）
・BIOS パスワードとスマートカード認証の連携（→ P.74）

## 認証パターンの登録の確認

ログオン認証に使う認証デバイスと、複数の認証デバイスを使って認証する場合に設定する「認証方式」の組み合わせを認証パターンといいます。
認証パターンには、ドライバがインストールされている認証デバイスが自動的に登録され、一覧で表示されます。

1. **「環境設定」を起動します（→ P.34）。**
2. **「設定項目一覧」から「ログオン認証」をクリックします。**
   「認証パターン」が表示されます。

## 3 「キー設定」の「－」の右隣に「スマートカード」が表示されていることを確認します。

「スマートカード」以外の認証パターンが表示されている場合には、次の手順で認証パターンを変更します。

1. 「キー設定」が「－」の認証パターンをクリックして選択し、「編集」をクリックします。
   「認証パターンの追加／変更」が起動します。

2. 「第 1 認証デバイス」が「スマートカード」、「第 2 認証デバイス」が空白の組合せをクリックして「OK」をクリックします。

重要

▶スマートカードホルダーをセットせずに SMARTACCESS をインストールすると、「認証パターン」に「スマートカード」が登録されません。その場合は、いったんSMARTACCESSをアンインストールしてからスマートカードホルダーを取り付け、再度SMARTACCESSをインストールしてください。

複数の認証デバイスをお使いになる場合、「認証パターン」より認証デバイスと順序を選択してから「認証方式」を選択して登録します。詳しくは、『リファレンスガイド』の「機能編」－「ログオン認証」－「認証パターンの設定」をご覧ください。

POINT

▶「認証方式」には「連携認証」と「連続認証」があります。
- 連携認証
  1 つ目のデバイスで認証し、その認証情報をもとに以降の認証を自動で行う認証方式です。
  「第 1 認証デバイス」が「スマートカード」、「第 2 認証デバイス」が「セキュリティチップ」の認証パターンの場合、スマートカードで認証を行うだけでユーザーキーパスワードを入力することなく認証できます。
- 連続認証
  認証パターンの順にすべての認証を行います。
  「第 1 認証デバイス」が「スマートカード」、「第 2 認証デバイス」が「セキュリティチップ」の認証パターンの場合、スマートカードで認証を行った後にユーザーキーパスワードを入力する必要があります。

▶「特定のキー」とは
認証時に「特定のキー」に設定したキーを押すことで、他の「認証パターン」に切り替えることができます。

・Windows Vista の場合
Windows ログオン時や「ユーザー情報設定」の起動時、【F9】キーに設定された「認証パターン」で認証ウィンドウが表示されます。
そのときに「特定のキー」で設定したキーを押すと、認証ウィンドウをその「特定のキー」に設定した認証パターンに切り替えることができます。
・Windows XP の場合
Windows ログオン時に「Windows へようこそ」ウィンドウから認証ウィンドウに切り替えるとき、または「ユーザー情報設定」の起動時、【Ctrl】+【Alt】+【Delete】に設定された「認証パターン」で認証ウィンドウが表示されます。
そのときに「特定のキー」で設定したキーを押すと、認証ウィンドウをその「特定のキー」に設定した認証パターンに切り替えることができます。

### 4 続けてアカウントの登録を行う場合は、「適用」をクリックします。

アカウントの登録を行う場合は、「アカウントの登録」（→ P.66）をご覧ください。

**POINT**

▶「環境設定」を終了するには、「OK」をクリックします。再起動を要求するメッセージが表示された場合は、Windows を再起動して設定を有効にします。

## アカウントの登録

SMARTACCESS を利用する管理者や利用者のアカウントは、「管理者ウィザード」で登録します。

### 1 「環境設定」を起動します（→ P.34）。

### 2 「設定項目一覧」から「ユーザー情報管理」をクリックします。

### 3 「アカウント追加」の「起動」をクリックします。

■ Windows Vista の場合
「ユーザーアカウント制御」ウィンドウが表示された場合は、開始されるプログラムを確認し、「続行」をクリックします。
「管理者ウィザード」ウィンドウが表示されます。
■ Windows XP の場合
「管理者ウィザード」ウィンドウが表示されます。

## 4 表示されている「認証の種類」と「認証デバイス」を確認し、「次へ」をクリックします。

「SMARTACCESS アカウントの登録」が表示されます。

## 5 SMARTACCESS で使用するアカウントを登録します。

複数の認証デバイスを使用する場合、「アカウント名」、「パスワード」は認証デバイスごとの制約をすべて満たすものを設定します。
他の認証デバイスの制約については、その認証デバイスの「アカウントの登録」のページをご覧ください。

**・アカウント名**

個人を識別するアカウントを入力します。
- 文字数や使用文字の制限はありません。
- 重複するユーザー名を使用することができます。

**・パスワード**

1 ～ 16 文字の半角英数字と記号で入力します。このパスワードが PIN となります。
「ポリシー」の「複雑さの設定」を設定している場合は、その設定内容に従って入力します。
「複雑さの設定」については『リファレンスガイド』の「ツール編」－「環境設定」－「ポリシー」－「スマートカード」をご覧ください。

**・パスワードの確認入力**

確認として「パスワード」で入力したものと同じ内容を入力します。

## 6 「次へ」をクリックします。

「Windows ユーザーの登録」が表示されます。

## 7 Windows ユーザーを登録します。

・Windows ユーザー名
「Windows ユーザー名」の右の▼をクリックして Windows アカウントを選択します。
ドメインに参加している場合、「ドメイン」を選択してから「Windows ユーザー名」の右の▼をクリックするとそのドメイン内の Windows アカウントを選択できます。
「Windows ユーザー名」に「ドメイン ¥Windows ユーザー名」とは入力しないでください。Windows ユーザー名とドメイン名は、それぞれの項目に分けて入力してください。
設定できるのは半角 20 文字まで、全角を使用する場合は 6 文字までです。

・ドメイン
ドメインに参加している場合は、「ドメイン」の▼をクリックしてドメインを選択します。

・パスワード
「Windows ユーザー名」で選択した Windows アカウントに登録されているパスワードを入力します。設定できるのは 14 文字までです。

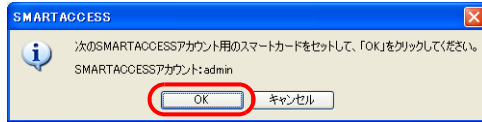
・パスワード入力確認
確認として「パスワード」と同じ内容を入力します。

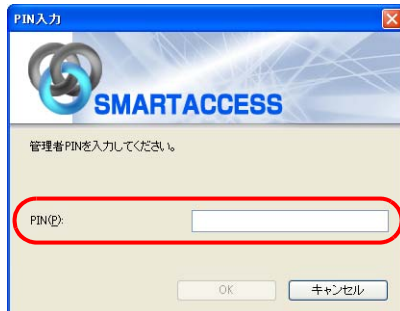
## 8 「次へ」をクリックします。

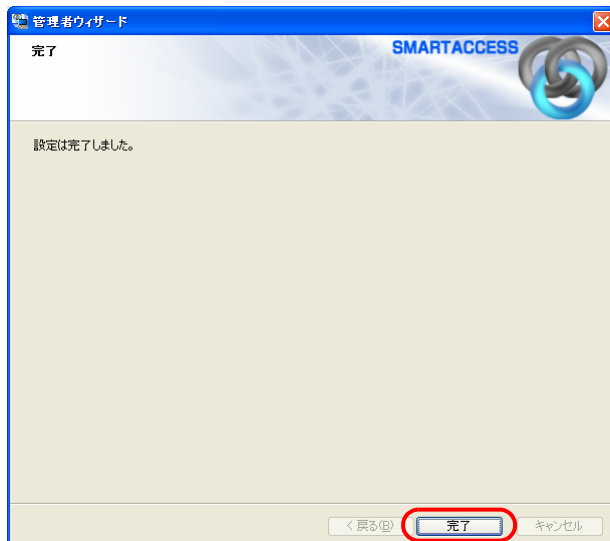
「設定の確認」が表示されます。

## 9 「設定内容」を確認し、「次へ」をクリックします。

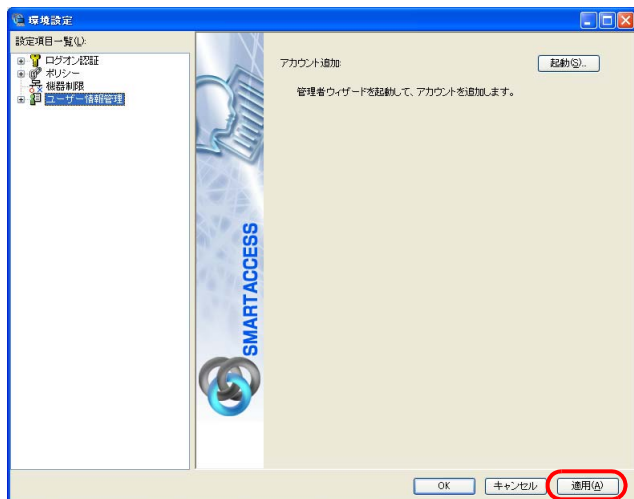
カードのセットを要求するウィンドウが表示されます。

## 10 リーダ／ライタにカードをセットします。

管理者 PIN による認証ウィンドウが表示されます。
スマートカードをリーダ／ライタにセットしたら、認証処理が終了するまではカードを抜かないでください。

## 11 「administrator」と入力して「OK」をクリックします。

「完了」と表示されます。

## 12 「完了」をクリックします。

「環境設定」に戻ります。

**13** **続けて Windows ログオンの設定を行う場合は、「適用」をクリックします。**

Windows ログオンの設定を行う場合は、「Windows ログオンの設定」（→ P.70）をご覧ください。

**POINT**

- 「環境設定」を終了するには、「OK」をクリックします。再起動を要求するメッセージが表示された場合は、Windows を再起動して設定を有効にします。

## Windows ログオンの設定

ここでは、Windows のログオン認証を、従来の Windows パスワードの認証から SMARTACCESS を使った認証に変更する手順を説明します。
Windows ログオンに関連する他の機能については『リファレンスガイド』の「機能編」－「ログオン認証」－「Windows ログオン」をご覧ください。

### ■Windows ログオンを有効にする

Windows ログオンを利用するには、「SMARTACCESS による Windows ログオン」を有効にします。

**1** **「環境設定」を起動します（→ P.34）。**

**2** **「設定項目一覧」から「ログオン認証」→「Windows ログオン」の順にクリックします。**

**3** **「SMARTACCESS による Windows ログオン」の「する」をクリックします。**

**4** **「OK」をクリックして「環境設定」を終了します。**
再起動を要求するメッセージが表示された場合は、Windows を再起動して設定を有効にします。

# カード操作によるコンピュータのロック

詳しくは『リファレンスガイド』の「機能編」－「ログオン認証」－「カードのポーリング動作」をご覧ください。

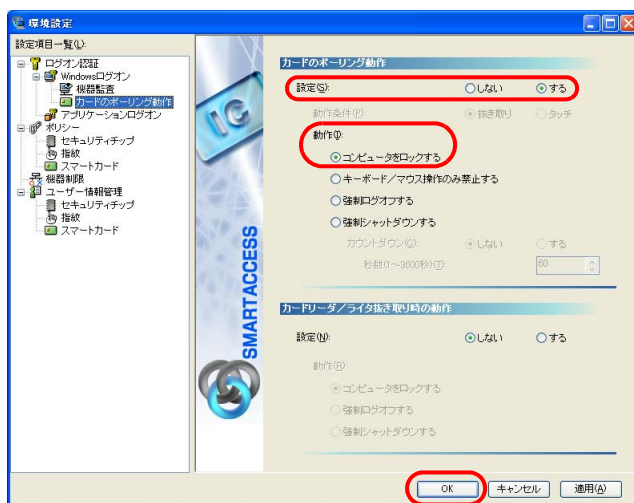
## ■「カードのポーリング動作」の設定をする

**重要**

- あらかじめ認証パターンに「スマートカード」を含む組み合わせを設定し、「SMARTACCESS による Windows ログオン」を「する」に設定してください。

**1** **「環境設定」を起動します（→ P.34）。**

**2** **「設定項目一覧」から「ログオン認証」→「Windows ログオン」→「カードのポーリング動作」をクリックします。**
「カードのポーリング動作」の詳細が表示されます。

**3** **次の項目を設定し、「OK」をクリックします。**
・「カードのポーリング動作」－「設定」
「する」をクリックします。
・「動作」
「コンピュータをロックする」をクリックします。

**重要**

- 「カードのポーリング動作」を「強制ログオフする」または「強制シャットダウンする」に設定している場合は、Windows のアクティブデスクトップ機能を利用しないでください。

## ■コンピュータのロックと解除

カードのポーリング動作を設定すると、スマートカードを利用して Windows ログオンした後は、スマートカードを抜き取るだけでコンピュータをロックすることができます。
コンピュータのロックを解除する場合は、次の操作を行います。

### □Windows Vista をお使いの場合

カードをセットして PIN を入力します。

### □Windows XP をお使いの場合

【Ctrl】+【Alt】+【Delete】キーを押します。認証画面が表示されるので、カードをセットして PIN を入力します。

## パスワードの変更

### ■PIN を変更する

利用者が PIN の変更をすることで、PIN を知っているのは利用者本人だけになります。セキュリティを強化するためにも、SMARTACCESS 運用開始時に利用者自身で PIN を変更することをお勧めします。

**1 「スタート」ボタン→「すべてのプログラム」→「SMARTACCESS」→「ユーザー情報設定」の順にクリックします。**

「ユーザー情報設定」ウィンドウの認証画面が表示されます。

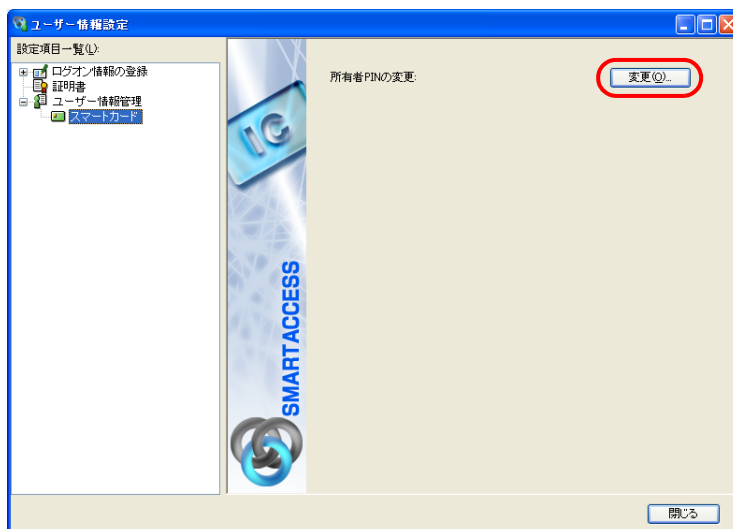
**2 リーダ／ライタにカードをセットし、PIN を入力します。**

認証されると「ユーザー情報設定」が起動します。

スマートカードをリーダ／ライタにセットしたら、認証処理が終了するまではカードを抜かないでください。

**3 「設定項目一覧」から「ユーザー情報管理」→「スマートカード」の順にクリックします。**

スマートカードのユーザー設定画面が表示されます。

**4 「変更」をクリックします。**

「所有者 PIN の変更」ウィンドウが表示されます。

### 5 「古い PIN」、「新しい PIN」および「新しい PIN の確認入力」を入力します。

・古い PIN
現在スマートカードに登録されている所有者 PIN を入力します。
・新しい PIN
変更後の所有者 PIN を、1 ～ 16 文字の半角英数字と記号で入力します。
「ポリシー」で複雑さの設定を行っている場合はその設定に従って入力します。
「複雑さの設定」については『リファレンスガイド』の「ツール編」－「環境設定」－「ポリシー」－「スマートカード」をご覧ください。
・新しい PIN の確認入力
確認として「新しい PIN」と同じ内容を入力します。

### 6 「OK」をクリックします。

「ユーザー情報設定」ウィンドウに戻ります。

### 7 「閉じる」をクリックして、「ユーザー情報設定」を終了します。

## スマートカードで Windows にログオンする

### 1 コンピュータを起動します。

■ Windows Vista をお使いの場合
「Windows へログオン」ウィンドウが表示されます。
手順 3 に進んでください。
■ Windows XP をお使いの場合
「Windows へようこそ」ウィンドウが表示されます。

### 2 【Ctrl】＋【Alt】＋【Delete】キーを押します。

「Windows へログオン」ウィンドウが表示されます。

### 3 リーダ／ライタにカードをセットし、PIN を入力します。

認証が行われ、Windows にログオンします。
スマートカードをリーダ／ライタにセットしたら、認証処理が終了するまではカードを抜かないでください。

## BIOS パスワードとスマートカード認証の連携

コンピュータ（BIOS）の起動時や BIOS セットアップの起動時にパスワードを入力する代わりに、スマートカード認証を使うことができます。
BIOS パスワードとの連携機能は、この機能に対応しているコンピュータでのみお使いになれます。

**1 コンピュータを起動します。**
「スマートカードが挿入されていません。スマートカードを挿入してください。」と表示されます。

**2 スマートカードをセットし、【Enter】キーを押します。**
「スマートカードの PIN を入力してください。」と表示されます。

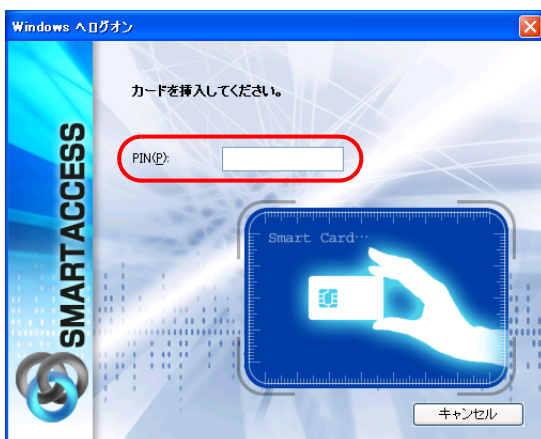
**3 BIOS ロックパスワード（→ P.74）を入力し、【Enter】キーを押します。**
認証が行われるとコンピュータが起動します。
「SMARTACCESS による Windows ログオン」を「する」に設定している場合は、しばらくすると Windows へのログオンウィンドウが表示されます。設定されている認証デバイスで認証を行うと、Windows にログオンします。スマートカードの場合、BIOS と Windows ログオンのシングルサインオン機能はありません。

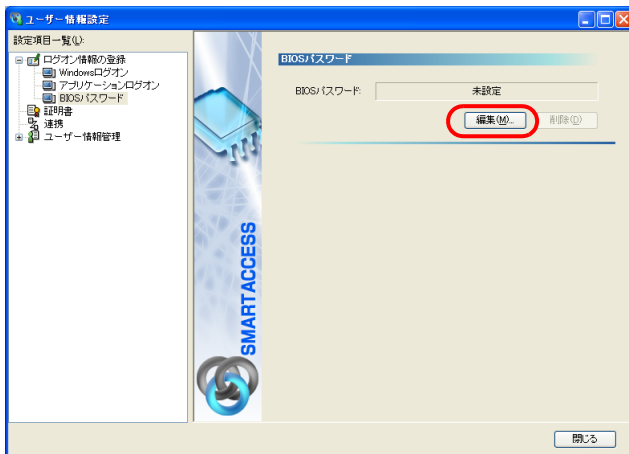
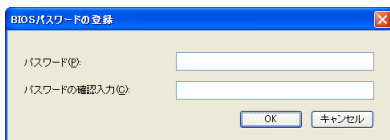
設定手順は次のとおりです。

### ■スマートカードに BIOS ロック用パスワードを登録する

初めてスマートカードによる BIOS ロック機能をお使いになる場合は、次の手順に従って登録してください。

**1 管理者用スマートカード、利用者用スマートカードを作成する**
「アカウントの登録」（→ P. 66）をご覧になり、管理者用および利用者用スマートカードを作成します。
・BIOS ロック用パスワードは、1 枚のカードに 1 つのパスワードしか設定できません。
　BIOS で管理者用パスワードとユーザー用パスワードを別に設定する場合は、スマートカードを複数用意し、それぞれのパスワードを登録してください。
　ユーザー用パスワードの設定は、管理者用パスワードを設定してからでないと行うことができません。管理者用スマートカードを作成した後、利用者用を作成してください。
・SMARTACCESS で「管理者 PIN」および「利用者 PIN」を変更する場合は、1 ～ 16 桁の半角英数字を使用してください。

**2 スマートカードに BIOS ロック用パスワードを登録する**
1. 「スタート」ボタン→「すべてのプログラム」→「SMARTACCESS」→「ユーザー情報設定」の順にクリックします。
「ユーザー情報設定」ウィンドウの認証画面が表示されます。
2. リーダ／ライタにカードをセットし、PIN を入力します。

認証されると「ユーザー情報設定」が起動します。
スマートカードをリーダ／ライタにセットしたら、認証処理が終了するまではカードを抜かないでください。

3. 「設定項目一覧」から「ユーザー情報管理」→「ログオン情報の登録」→「BIOS パスワード」の順にクリックします。
BIOS パスワードの設定画面が表示されます。
4. 「編集」をクリックします。

「BIOS パスワードの登録」ウィンドウが表示されます。
5. 次の項目に入力し、「OK」をクリックします。

・ パスワード
BIOS パスワードを入力します。
1 ～ 14 文字の半角英数字（a ～ z、A ～ Z、0 ～ 9）で入力します。なお、スマートカードには大文字と小文字を区別して記録されますが、BIOS では大文字と小文字は区別されません。
半角英数字以外の文字をお使いになると、コンピュータが起動できなくなります。
詳しくは、『リファレンスガイド』の「ツール編」－「ユーザー情報設定」－「ログオン情報の登録」－「BIOS パスワード」をご覧ください。

## ■コンピュータ本体の BIOS の設定を変更する

コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧になり、次の設定を行ってください。
スマートカードホルダーをお使いの場合、コンピュータ本体にスマートカードホルダーをセットしてからコンピュータを起動してください。スマートカードホルダーをセットしていないと、BIOS セットアップに「スマートカードによるロック」の項目が表示されません。

### 1 BIOS セットアップの「管理者用パスワード」に管理者用スマートカードに登録した BIOS ロック用パスワードと同じパスワードを登録します。

必ずスマートカードに BIOS ロック用パスワードを登録してから、BIOS の設定を変更してください。
BIOS ロック用パスワードを登録せずに BIOS の設定を変更すると、コンピュータが起動できなくなります。

### 2 「ユーザー用パスワード」に利用者用スマートカードに登録した BIOS ロック用パスワードと同じパスワードを登録します。

### 3 スマートカードによるロックを使用する設定にします。

## ■BIOS ロック用パスワードを変更する

スマートカードに登録した BIOS ロック用パスワードを変更する場合は、次の手順に従って変更してください。

### 1 コンピュータ本体の BIOS の設定を変更する

コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧になり、BIOS セットアップでスマートカードによるロックを使用しない設定にしてください。

### 2 管理者用スマートカードまたはユーザー用スマートカードの BIOS ロック用パスワードを変更する

変更方法については、『リファレンスガイド』の「ツール編」－「ユーザー情報設定」－「ログオン情報の登録」－「BIOS パスワード」をご覧ください。

## ■コンピュータ（BIOS）起動時の注意事項

PIN を連続して 15 回間違えて入力すると、カードがロックされ使用できなくなります。
ロックされたスマートカードではコンピュータにログオンできなくなるので、PIN は忘れないようにしてください。

# 5 セキュリティチップをお使いの場合

ここでは、セキュリティチップと SMARTACCESS を使って Windows へのログオン時の認証を行うための設定について説明します。

## ■設定の流れ

### □管理者による設定

1 認証パターンの登録の確認（→ P.77）

2 アカウントの登録（→ P.79）

3 Windows ログオンの設定（→ P.82）

### □利用者による設定

4 パスワードの変更（→ P.83）

## ■ログオン手順

・セキュリティチップのユーザーキーパスワードで Windows にログオンする（→ P.85）

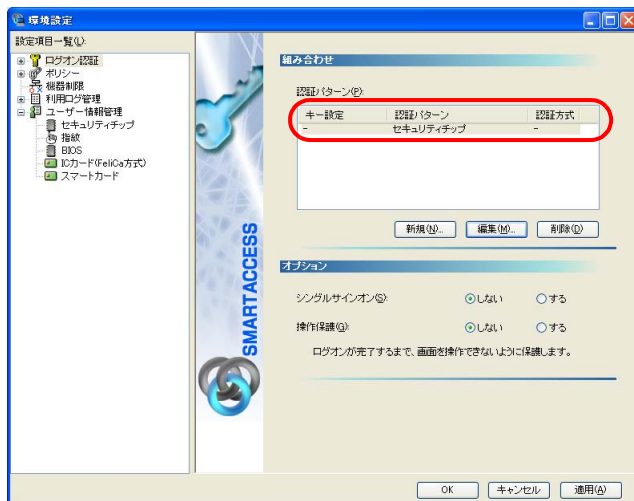
## 認証パターンの登録の確認

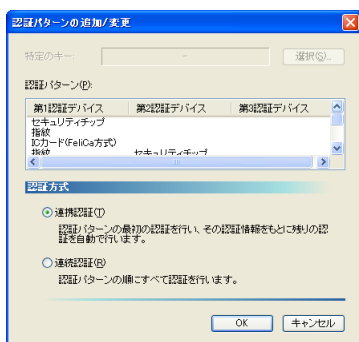
ログオン認証に使う認証デバイスと、複数の認証デバイスを使って認証する場合に設定する「認証方式」の組み合わせを認証パターンといいます。
認証パターンには、ドライバがインストールされている認証デバイスが自動的に登録され、一覧で表示されます。

1 「環境設定」を起動します（→ P.34）。

2 「設定項目一覧」から「ログオン認証」をクリックします。

「認証パターン」が表示されます。

3 「キー設定」の「－」の右隣に「セキュリティチップ」が表示されていることを確認します。

「セキュリティチップ」以外の認証パターンが表示されている場合には、次の手順で認証パターンを変更します。

1. **「キー設定」が「−」の認証パターンをクリックして選択し、「編集」をクリックします。**
   「認証パターンの追加／変更」が起動します。

2. **「第 1 認証デバイス」が「セキュリティチップ」、「第 2 認証デバイス」が空白の組合せをクリックして「OK」をクリックします。**

複数の認証デバイスをお使いになる場合、「認証パターン」より認証デバイスと順序を選択してから「認証方式」を選択して登録します。詳しくは、『リファレンスガイド』の「機能編」―「ログオン認証」―「認証パターンの設定」をご覧ください。

**POINT**

▶「認証方式」には「連携認証」と「連続認証」があります。
- 連携認証
  1 つ目のデバイスで認証し、その認証情報をもとに以降の認証を自動で行う認証方式です。
  「第 1 認証デバイス」が「指紋」、「第 2 認証デバイス」が「セキュリティチップ」の認証パターンの場合、指紋認証を行うだけでユーザーキーパスワードを入力することなく認証できます。
- 連続認証
  認証パターンの順にすべての認証を行います。
  「第 1 認証デバイス」が「指紋」、「第 2 認証デバイス」が「セキュリティチップ」の認証パターンの場合、指紋認証を行った後にユーザーキーパスワードを入力する必要があります。

▶「特定のキー」とは
認証時に「特定のキー」に設定したキーを押すことで、他の「認証パターン」に切り替えることができます。
- Windows Vista の場合
  Windows ログオン時や「ユーザー情報設定」の起動時、【F9】キーに設定された「認証パターン」で認証ウィンドウが表示されます。
  そのときに「特定のキー」で設定したキーを押すと、認証ウィンドウをその「特定のキー」に設定した認証パターンに切り替えることができます。
- Windows XP の場合
  Windows ログオン時に「Windows へようこそ」ウィンドウから認証ウィンドウに切り替えるとき、または「ユーザー情報設定」の起動時、【Ctrl】+【Alt】+【Delete】に設定された「認証パターン」で認証ウィンドウが表示されます。
  そのときに「特定のキー」で設定したキーを押すと、認証ウィンドウをその「特定のキー」に設定した認証パターンに切り替えることができます。

## 4 続けてアカウントの登録を行う場合は、「適用」をクリックします。

アカウントの登録を行う場合は、「アカウントの登録」(→ P.79)をご覧ください。

**POINT**

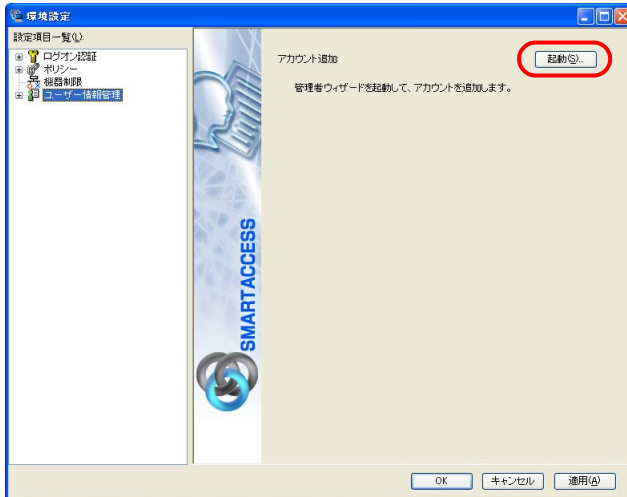
▶「環境設定」を終了するには、「OK」をクリックします。再起動を要求するメッセージが表示された場合は、Windows を再起動して設定を有効にします。

## アカウントの登録

SMARTACCESS を利用する管理者や利用者のアカウントは、「管理者ウィザード」で登録します。

**1** **「環境設定」を起動します（→ P.34）。**

**2** **「設定項目一覧」から「ユーザー情報管理」をクリックします。**

**3** **「アカウント追加」の「起動」をクリックします。**

■ Windows Vista の場合
「ユーザーアカウント制御」ウィンドウが表示された場合は、開始されるプログラムを確認し、「続行」をクリックします。
「管理者ウィザード」ウィンドウが表示されます。

■ Windows XP の場合
「管理者ウィザード」ウィンドウが表示されます。

**4** **表示されている「認証の種類」と「認証デバイス」を確認し、「次へ」をクリックします。**

「SMARTACCESS アカウントの登録」が表示されます。

## 5 SMARTACCESS で使用するアカウントを登録します。

複数の認証デバイスを使用する場合、「アカウント名」、「パスワード」は認証デバイスごとの制約をすべて満たすものを設定します。
他の認証デバイスの制約については、その認証デバイスの「アカウントの登録」のページをご覧ください。

**・アカウント名**

手順 7 で選択する「Windows ユーザー名」と同じ内容を入力します。

- 文字数や使用文字の制限はありません。
- 重複するユーザー名を使用することができます。

**・パスワード**

6 ～ 256 文字の半角英数字と記号で入力します。このパスワードがユーザーキーパスワードとなります。
「ポリシー」の「複雑さの設定」を設定している場合は、その設定内容に従って入力します。
「複雑さの設定」については『リファレンスガイド』の「ツール編」－「環境設定」－「ポリシー」－「セキュリティチップ」をご覧ください。

**・パスワードの確認入力**

確認として「パスワード」で入力したものと同じ内容を入力します。

## 6 「次へ」をクリックします。

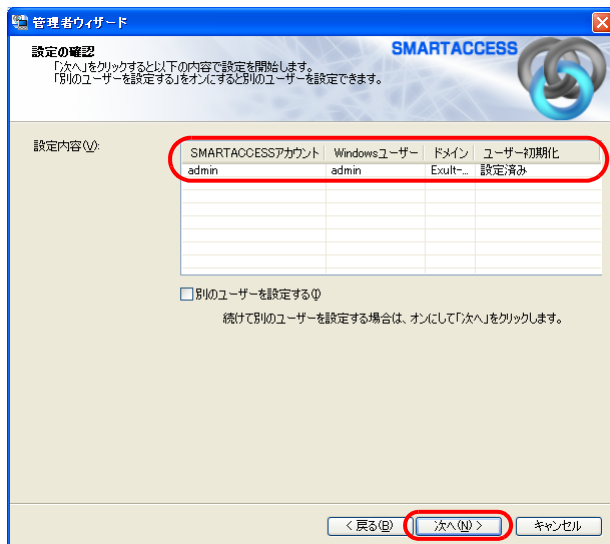
「Windows ユーザーの登録」が表示されます。

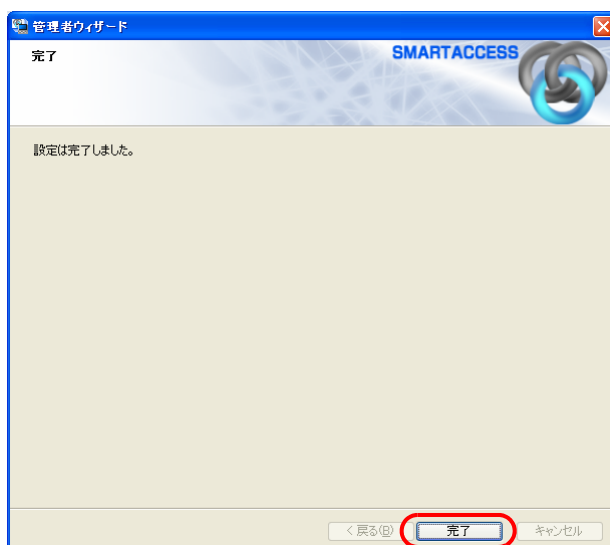
## 7 Windows ユーザーを登録します。

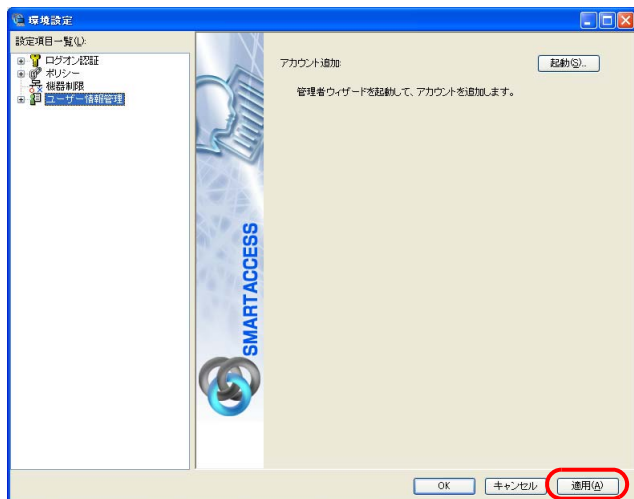
・Windows ユーザー名
「Windows ユーザー名」の右の▼をクリックして Windows アカウントを選択します。
ドメインに参加している場合、「ドメイン」を選択してから「Windows ユーザー名」の右の▼をクリックするとそのドメイン内の Windows アカウントを選択できます。
「Windows ユーザー名」に「ドメイン ¥Windows ユーザー名」とは入力しないでください。Windows ユーザー名とドメイン名は、それぞれの項目に分けて入力してください。
セキュリティチップを使って Windows ログオン認証をするときに入力する「Windows ユーザー名」となります。
・ドメイン
ドメインに参加している場合は、「ドメイン」の▼をクリックしてドメインを選択します。
・パスワード
「Windows ユーザー名」で選択した Windows アカウントに登録されているパスワードを入力します。
・パスワード入力確認
確認として「パスワード」と同じ内容を入力します。

## 8 「次へ」をクリックします。

「設定の確認」が表示されます。

## 9 「次へ」をクリックします。

「完了」と表示されます。

## 10 「完了」をクリックします。

「環境設定」に戻ります。

**11** **続けて Windows ログオンの設定を行う場合は、「適用」をクリックします。**

Windows ログオンの設定を行う場合は、「Windows ログオンの設定」（→ P.82）をご覧ください。

**POINT**

- 「環境設定」を終了するには、「OK」をクリックします。再起動を要求するメッセージが表示された場合は、Windows を再起動して設定を有効にします。

## Windows ログオンの設定

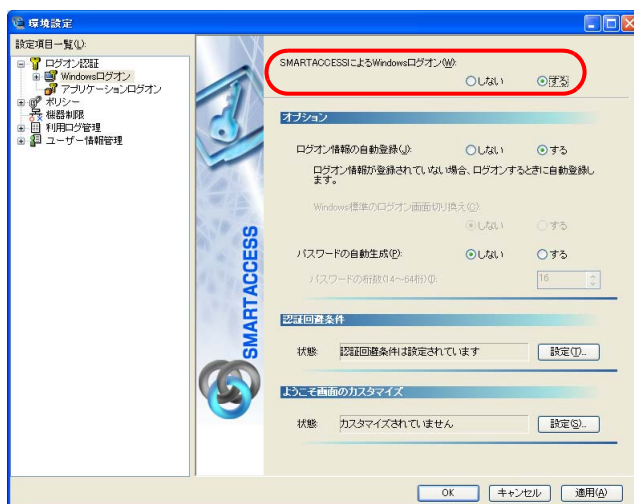
ここでは、Windows のログオン認証を、従来の Windows パスワードの認証から SMARTACCESS を使った認証に変更する手順を説明します。
Windows ログオンに関連する他の機能については『リファレンスガイド』の「機能編」－「ログオン認証」－「Windows ログオン」をご覧ください。

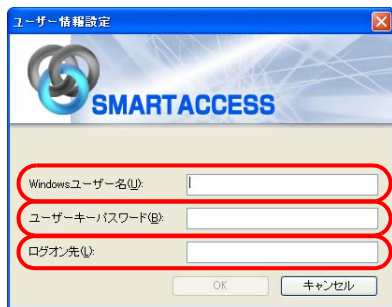
### ■Windows ログオンを有効にする

Windows ログオンを利用するには、「SMARTACCESS による Windows ログオン」を有効にします。

**1** **「環境設定」を起動します（→ P.34）。**

**2** **「設定項目一覧」から「ログオン認証」→「Windows ログオン」の順にクリックします。**

**3** **「SMARTACCESS による Windows ログオン」の「する」をクリックします。**

**4** **「OK」をクリックして「環境設定」を終了します。**

再起動を要求するメッセージが表示された場合は、Windows を再起動して設定を有効にします。

# パスワードの変更

## ■ユーザーキーパスワードを変更する

利用者がユーザーキーパスワードの変更をすることで、ユーザーキーパスワードを知っているのは利用者本人だけになります。セキュリティを強化するためにも、SMARTACCESS 運用開始時に利用者自身でユーザーキーパスワードを変更することをお勧めします。

**1** **「スタート」ボタン→「すべてのプログラム」→「SMARTACCESS」→「ユーザー情報設定」の順にクリックします。**

「ユーザー情報設定」ウィンドウの認証画面が表示されます。

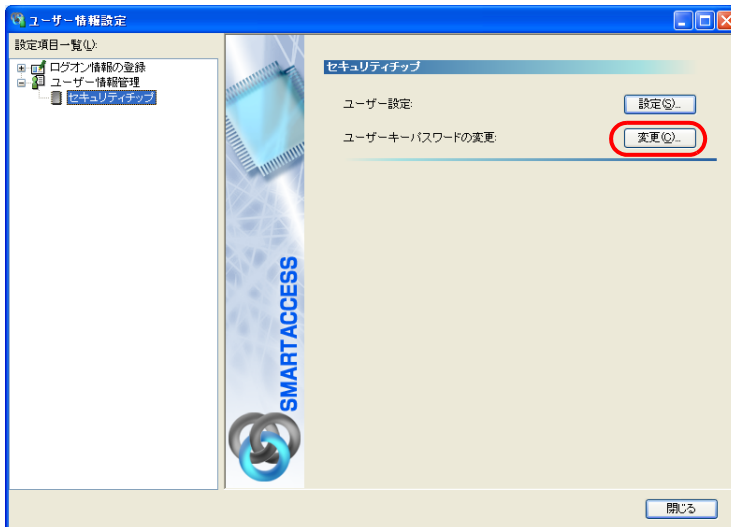
**2** **Windows ユーザー名とユーザーキーパスワードを入力します。ドメインに参加している場合は、ログオン先も入力します。**

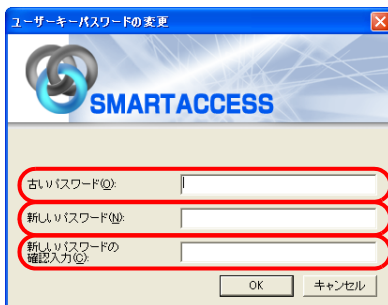
- **Windows ユーザー名**
  ユーザーキーパスワードを変更する Windows ユーザー名を入力します。
- **ユーザーキーパスワード**
  ユーザーキーパスワードを入力します。
- **ログオン先**
  ドメインに参加している場合、ログオン先のドメイン名を入力します。

認証されると「ユーザー情報設定」が起動します。

**3** **「設定項目一覧」から「ユーザー情報管理」→「セキュリティチップ」の順にクリックします。**

セキュリティチップのユーザー設定画面が表示されます。

## 4 「変更」をクリックします。

「ユーザーキーパスワードの変更」ウィンドウが表示されます。

## 5 「古いパスワード」、「新しいパスワード」および「新しいパスワードの確認入力」に入力します。

- **古いパスワード**
  現在のユーザーキーパスワードを入力します。
- **新しいパスワード**
  変更後のユーザーキーパスワードを、6 ～ 256 文字の半角英数字と記号で入力します。
  「ポリシー」で複雑さの設定を行っている場合はその設定に従って入力します。
- **新しいパスワードの確認入力**
  確認として「新しいパスワード」と同じ内容を入力します。

## 6 「OK」をクリックします。

「ユーザー情報設定」ウィンドウに戻ります。

## 7 「閉じる」をクリックして、「ユーザー情報設定」を終了します。

# セキュリティチップのユーザーキーパスワードで Windows にログオンする

## 1 コンピュータを起動します。

■ Windows Vista をお使いの場合

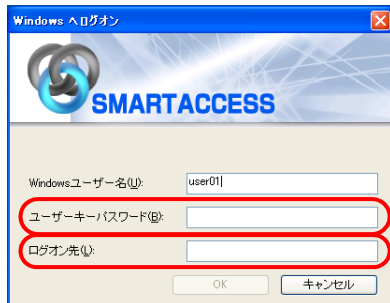
「Windows へログオン」ウィンドウが表示されます。
手順 3 に進んでください。

■ Windows XP をお使いの場合

「Windows へようこそ」ウィンドウが表示されます。

## 2 【Ctrl】+【Alt】+【Delete】キーを押します。

「Windows へログオン」ウィンドウが表示されます。

## 3 ユーザーキーパスワードを入力します。ドメインに参加している場合は、ログオン先にドメイン名を入力します。

## 4 「OK」をクリックします。

認証が行われ、Windows にログオンします。

第 5 章

# 認証デバイスの取り扱い

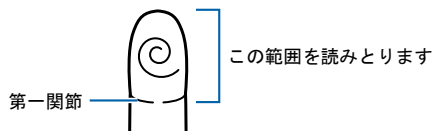
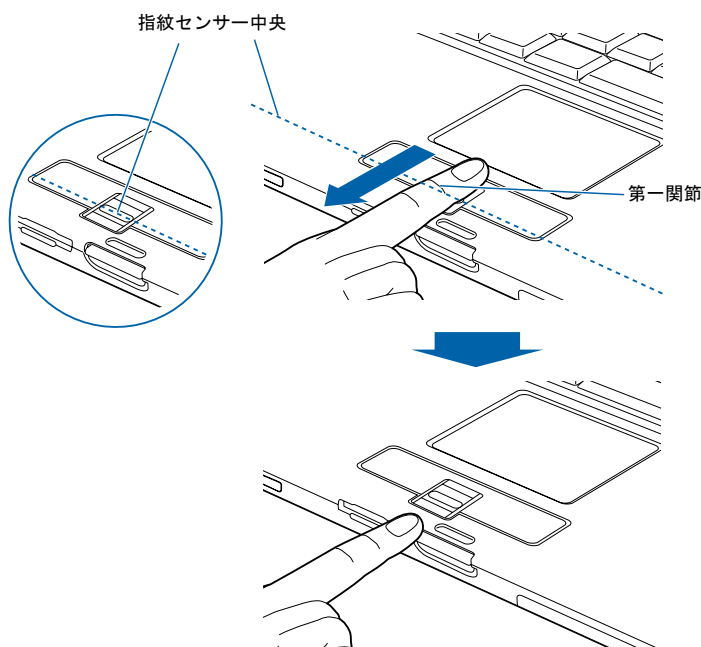
認証デバイスをお使いになるための注意事項や基本的な取り扱い方について説明しています。

# 1 指紋センサー

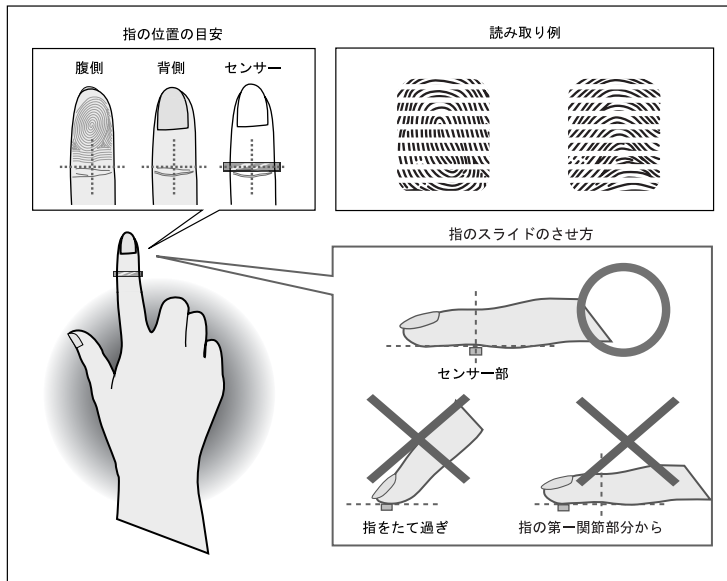
## 指紋の読み取り方

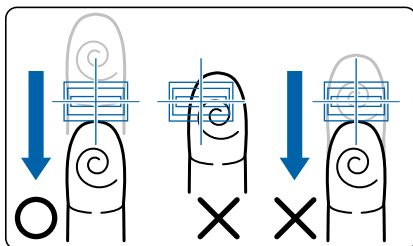
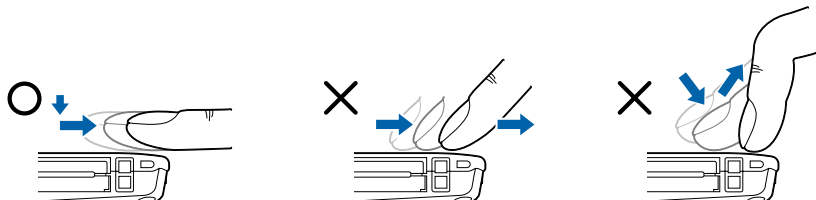
指紋の登録や認証を行う場合は、次のように指をスライドさせてください。認証の失敗を減らすことができます。

**1 操作する指の第一関節が、指紋センサーの中央部に来るように準備します。**

第一関節より先の部分が読み取り範囲となります。

**2 指をまっすぐ伸ばして、第一関節を指紋センサーに軽く当てます。続いて手全体を引くようにして、センサー部が完全に見えるまでスライドさせます。**

（イラストは機種や状況により異なります）

## ■指のスライドのさせ方について

正しく指紋を読み取らせるため、次の図のように指を置いてください。

### 重要

- うまく認識されないときは
  次の点に気を付けて操作してください。
  ・指の第一関節より先の部分が、指紋センサー上を通過するようにする
  ・指紋の渦の中心が、指紋センサーの中心を通過するようにする
  ・1 秒程度で通過するくらいの速さで、スーッと動かす

  なお、親指など、指紋の渦の中心を合わせにくい指は、うまく認識できないことがあります。その際は、中心を通過させやすい指を登録してください。
- 指を突き立てたり、引っかけるようにスライドさせないでください。
  指紋センサーに指のはら（指紋の中心部）が接触していなかったり、指を引っかけるようにスライドさせると指紋の読み取りがうまくいかない場合があります。
  必ず、指のはら（指紋の中心部）が指紋センサーに接触するようにスライドさせてください。

（イラストは機種や状況により異なります）

- 指紋の読み取りがうまくいかない場合
  指のスライドが速すぎたり遅すぎたりした場合、正常に認識できないことがあります。画面のメッセージに従って、スライドの速さを調節してください。

# 取り扱い上の注意事項

## ■指紋登録時／照合時のご注意

・指紋の登録や照合を行うときには、「指紋の読み取り方」（→ P.88）をご覧になり、指紋センサー上で正しく指をスライドさせてください。指が正しく置かれていないと、指紋を読み取ることが困難になったり、照合率が低下したりすることがあります。
・指の状態が次のような場合には、指紋の登録が困難になったり、照合率が低下することがあります。
　- 汗や脂が多い
　- 手が荒れたり、極端に乾燥している
　- 指に傷がある、または磨耗して指紋が薄い
　- 急に太ったり、やせたりして指紋が変化した
　手を洗う、手を拭く、登録する指を変えるなどお客様の指の状態に合わせて対処することで、登録時や照合時の状況が改善されることがあります。
・指紋の読み取りを行う前に金属に手を触れるなどして、静電気を取り除いてください。静電気が故障の原因となる場合があります。冬季など乾燥する時期は特にご注意ください。

## ■センサーに関するご注意

・センサー部分をひっかいたり、先のとがったもので押したりしないでください。傷により発熱する原因となります。
・使用中にセンサー表面が温かくなることがありますが、故障ではありません。

## ■センサー表面の清掃について

・指紋センサーのセンサー部は直接指で触れる部分であるため、汚れやすくなっています。
　センサー表面が汚れていると、指紋の読み取りが困難になったり、照合率が低下したりすることがありますので、ときどき清掃を行ってください。清掃の際には、乾いたやわらかい布でセンサー表面の汚れを軽く拭き取ってください。
・清掃の際に、センサー表面に水などの液体をたらさないでください。また、ベンジンなどの揮発性有機溶剤や化学雑巾は使用しないでください。
・指紋の登録失敗や照合失敗が頻発するときには、センサー表面を清掃してください。

# 2 FeliCa 対応リーダ／ライタ

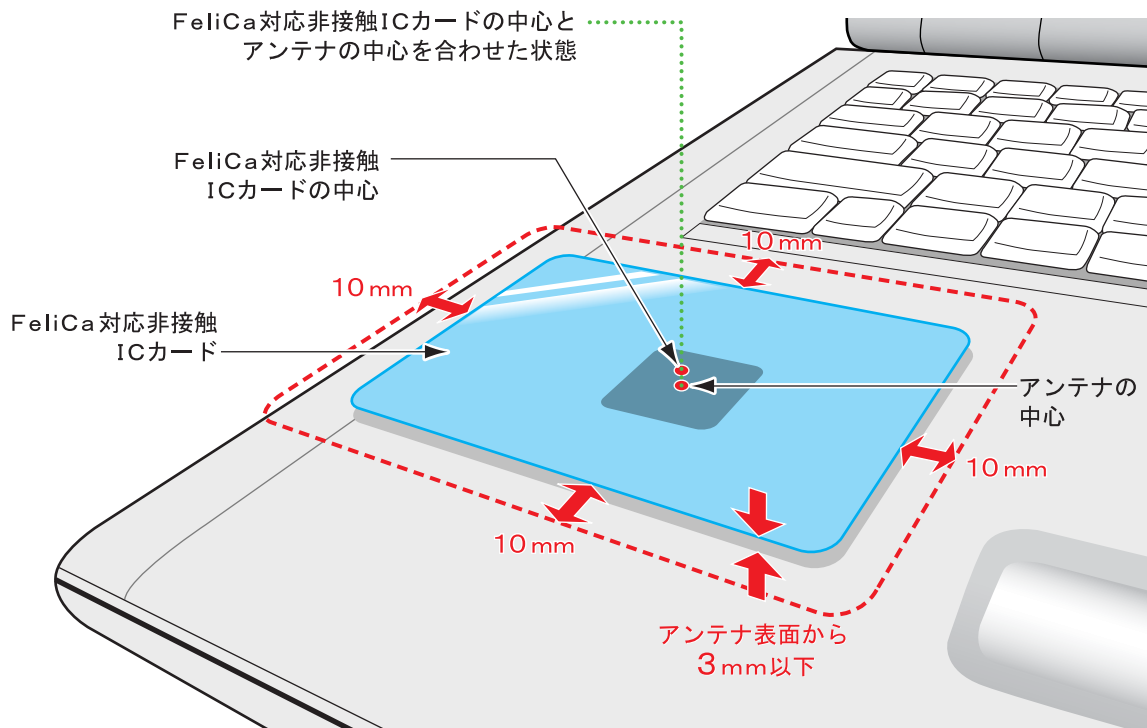
## カードの読み取りについて

コンピュータ本体に内蔵されている FeliCa 対応リーダ／ライタは、鉄道の改札機などのリーダ／ライタと比べると電波強度が弱いため、FeliCa 対応非接触 IC カードを認識できる範囲が限られます。良好な通信ができる範囲の目安は、次のとおりです（機種およびカードの種類によって若干異なります）。

**重要**

- お使いの機種によりアンテナの位置が異なります。アンテナの位置については、コンピュータ本体の『製品ガイド』の「各部名称」をご覧ください。

**POINT**

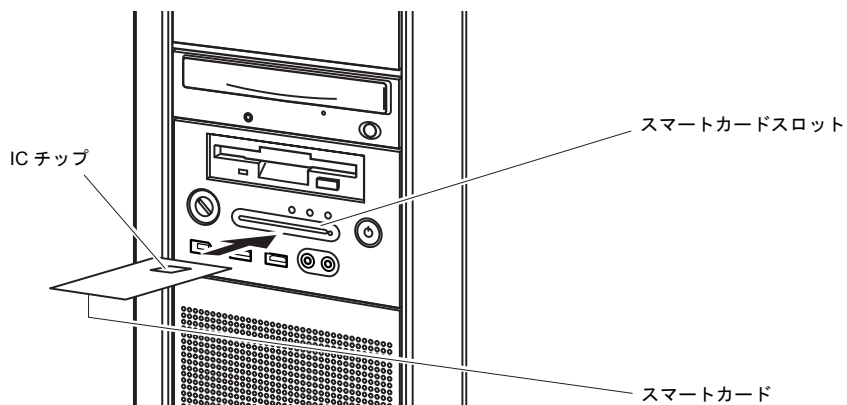
- アンテナ表面からの距離は、3mm 以下
- FeliCa 対応非接触 IC カードの中心とアンテナの中心を合わせた状態から、前後左右に 10mm 以内

## 注意事項

- SMARTACCESS では、外付けの FeliCa 対応リーダ／ライタ（PaSoRi）はサポートしておりません。
- FeliCa 対応非接触 IC カードについて
  FeliCa 対応リーダ／ライタには、認証に使用するための IC カードは添付されておりません。
  弊社純正品「FeliCa 対応非接触 IC カード（SMARTACCESS 専用）（FMFLC-C1）」を別途ご購入ください。
  なお、FeliCa 対応非接触 IC カードは SMARTACCESS 専用のカードです。カードにフォーマットを追加することができないため、他のソフトウェアや入退室管理システムなどのサービスにはご使用できません。

# 3 スマートカードリーダ／ライタ、スマートカードホルダー

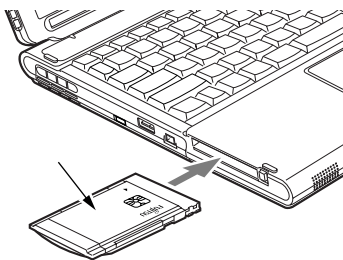
## 取り扱い方

### ■スマートカードリーダ／ライタ

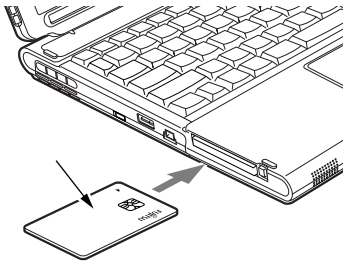
スマートカードは IC チップ面を上にして、奥までゆっくり差し込みます。
スマートカードリーダ／ライタの位置などについては、コンピュータ本体の『製品ガイド』の「各部名称」をご覧ください。

（イラストは機種や状況により異なります）

### ■スマートカードホルダー

#### □スマートカードホルダーをセットする

コンピュータ本体の電源が切れていること、スマートカードホルダーにスマートカードが差し込まれていないことを確認してから、「FUJITSU」のロゴがある面を上にして、コンピュータ本体のPCカードスロットにスマートカードホルダーをセットします。
PCカードスロットの位置や使い方については、コンピュータ本体の『製品ガイド』をご覧ください。

（イラストは機種や状況により異なります）

### □スマートカードをセットする

スマートカードは IC チップ面を上にして、スマートカードホルダーの奥までゆっくり差し込みます。

（イラストは機種や状況により異なります）

### □スマートカードを抜き取る

スマートカードを使用するソフトウェアの指示に従うか、ソフトウェアが終了していることを確認してからスマートカードを抜き取ります。

**重要**

- スマートカードがソフトウェアを使用しているときにスマートカードを抜き取ると、データが破壊されるおそれがあります。必ずソフトウェアの抜き取り指示に従うか、ソフトウェアが終了していることを確認してから抜き取ってください。

### □スマートカードホルダーを取り出す

コンピュータ本体の電源を切り、PC カードスロットからスマートカードホルダーを取り出します。
PC カードスロットから取り出す方法については、コンピュータ本体の『製品ガイド』をご覧ください。

## 取り扱い上の注意事項

### □スマートカードリーダ／ライタの注意事項

・スマートカードをセットしている状態からコンピュータを再起動するときは、「OK」または「はい」をクリックして再起動を実行してから、起動画面が出るまでの間に、スマートカードを取り出してください。

### □スマートカードホルダーの注意事項

・スマートカードホルダーは、コンピュータ本体の電源が入った状態でのセットまたは取り出しに対応しておりません。必ず、コンピュータ本体の電源を切った状態で行ってください。
・スマートカードホルダーをセットしたり取り出したりする場合は、必ずスマートカードを取り出しておいてください。
・スマートカードホルダーは、他のスマートカード読み取り装置と同時に使用することはできません。
・スマートカードホルダーは、IC チップを使用した大変デリケートな電子部品です。
落下などの衝撃を与えないでください。
・スタンバイや休止状態からレジューム（復帰）後、もう一度スタンバイや休止状態を行う場合は、しばらく（30 秒程度）待ってから操作してください。短い間隔で行うと、正しく動作しない場合があります。

### □カードの取り扱いについての注意事項

・スマートカードを使用するときは、次の点に注意してください。
- 折り曲げたり、汚したり、濡らしたりしないでください。
- 磁石などの磁気を帯びたものを近づけないでください。
- 電気を帯びたものを上に載せたり、近くで静電気を発生させたりしないでください。
- 高温の場所に保管しないでください。
- カードに衝撃を与えないでください。

・コンピュータを持ち運ぶ場合は、スマートカードを取り出しておいてください。

・他の装置で作成した、拡張情報の多いスマートカードの読み取りを行うと、ごくまれにスマートカードの機能が停止する場合があります。
このような場合、コンピュータを再起動してください。再起動後、スマートカードリーダ／ライタやスマートカードホルダーで作成したスマートカードをお使いになるか、拡張情報を減らした形式で作成し直したスマートカードをお使いください。

・寿命について
スマートカードは、カードに搭載されている IC チップを、スマートカードリーダ／ライタやスマートカードホルダー内部のソケットに接触させることによって、IC チップに内蔵されている情報の読み取り／書き込みを行います。そのため、同じスマートカードホルダー、スマートカードを長期間にわたって使用していると、IC チップやソケットなどの電子部品が消耗して、正しい情報の読み取り／書き込みができなくなってきます。保守作業として定期的にスマートカードホルダー、スマートカードを交換することをお勧めします。
なお、次の状態になった場合を交換の目安としてください。
- スマートカードをセットしても認識されなくなってきた場合
- スマートカードが読み取りにくくなってきた場合
- データの更新に時間がかかるようになってきた場合
スマートカードのご購入については、「富士通パーソナル製品に関するお問合せ窓口」、またはご購入元にお問い合わせください。

# 4 セキュリティチップ

## セキュリティチップの管理

セキュリティチップには、セキュリティチップの管理を行う「所有者」とセキュリティチップを使用する「ユーザ」を登録します。
「所有者」および「ユーザ」は次の鍵および証明書やファイルを作成・利用します。

**POINT**

- SMARTACCESS の「管理者」、「利用者」と Security Platform（Infineon TPM Professional Package）の関係は、次のようにしてお使いになることをお勧めします。

| SMARTACCESS | Security Platform（Infineon TPM Professional Package） |
|---|---|
| 管理者 | 所有者 |
| 利用者 | ユーザ |

### ■「所有者」が管理するもの

#### □所有者キーと所有者パスワード

所有者は、所有者であることを証明するキーを作成します。この鍵はセキュリティチップにより保護され、所有者パスワードを入力することによって利用することができます。所有者パスワードは忘れないよう注意してください。

#### □自動バックアップファイルと復元用トークン

セキュリティチップで管理しているすべての鍵や証明書のバックアップを行います。バックアップはスケジュールを設定することにより定期的に行うことができます。
セキュリティチップが故障しても、新しいコンピュータでこのファイルを用いて復元することにより、以前利用していた暗号化ファイルなどが利用できるようになります。
自動バックアップファイルは、トークンにより暗号化されています。自動バックアップファイルを利用する場合には、トークンファイルとそのパスワードが必要です。 トークンファイルを失くしたり、パスワードを忘れたりしないよう注意して管理してください。

#### □パスワードリセットファイルとリセットトークン

「ユーザ」がセキュリティチップのパスワードを忘れた場合に備えて、あらかじめパスワードリセット用のトークンを作成しておくことで現状のパスワードを新規パスワードに変更することができます。「所有者」はあらかじめパスワードリセットの設定を行い、必要に応じて「ユーザ」のパスワードを設定し直すことを許可します。

### ■「ユーザ」が管理するもの

#### □ユーザーキーとユーザーキーパスワード

「ユーザ」はセキュリティチップを利用する場合、ユーザーキーを作成します。このキーはセキュリティチップにより保護され、ユーザーキーパスワードを入力することによって利用することができます。キーを紛失した場合は、それ以前に暗号化していたデータやファイルなどを再び利用することができなくなります。管理には注意してください。また、パスワードを忘れた場合も、キーが利用できなくなるため、それまでに暗号化していたデータやファイルを再び利用することができなくなります。パスワードは忘れないよう注意してください。

#### □パスワードリセット 個人シークレット

「ユーザ」はセキュリティチップのパスワードを忘れた場合に備えて、あらかじめパスワードリセット用の個人シークレットを作成しておくことで現状のパスワードを新規パスワードに変更することができます。「ユーザ」はあらかじめパスワードリセットの設定を行い、必要に応じて「ユーザ」のパスワードを設定し直します。

## ■鍵や証明書、パスワードの管理について

セキュリティチップは、複数の鍵や証明書を扱います。これらの鍵や証明書を紛失した場合は、その鍵によって暗号化されたファイルなどは利用できなくなることがありますので注意してください。またこれらの鍵を利用する場合はパスワードが必要です。パスワードを正しく入力しないと鍵が利用できないため、紛失時と同様に暗号化されたファイルなどが利用できなくなります。

### □新しいユーザーを登録するには

Windows に新規ユーザーを追加する場合、そのユーザーがセキュリティチップを利用するためには、セキュリティチップに新規ユーザーの情報を登録する必要があります。SMARTACCESS では Windows へ新規ユーザーを追加し、セキュリティチップの登録を行うことができます。

### □パスワードの変更

セキュリティチップに設定した、所有者パスワードおよびユーザーキーパスワードは変更することができます。また、ユーザーキーパスワードは各ユーザで定期的に変更することをお勧めします。

・「所有者パスワード」の変更については、『リファレンスガイド』の「ツール編」－「環境設定」－「ユーザー情報管理」－「セキュリティチップ」をご覧ください。
・「ユーザーキーパスワード」の変更については、『リファレンスガイド』の「ツール編」－「ユーザー情報設定」－「ユーザー情報管理」－「セキュリティチップ」、および「環境設定」－「ユーザー情報管理」－「セキュリティチップ」をご覧ください。

### □パスワードを忘れた場合には

ユーザーキーパスワードを忘れた場合は、再設定することができます。

ユーザーキーパスワードを再設定する場合には、所有者が事前にパスワードリセットの設定を行う必要があります。

パスワードをリセットする場合は、『リファレンスガイド』の「ツール編」－「環境設定」－「ユーザー情報管理」－「セキュリティチップ」をご覧ください。

## 第 6 章

# こんなときには

おかしいなと思ったときや、わからないことがあったときの対処方法について説明しています。

# 1 運用上の注意

## 通常備えておくこと

次のような場合、SMARTACCESS の設定がリセットされてしまったり、認証デバイスが使えなくなったりすることがあります。

・コンピュータの故障時
・セキュリティチップの故障時
・ハードディスクのリカバリ後
・コンピュータの部品の交換後

このような場合に備えて、必ず SMARTACCESS の設定やセキュリティチップの鍵を定期的にバックアップをしてください。バックアップファイルやその時に設定したパスワードは、紛失したり忘れたりしないよう注意して管理してください。
セキュリティチップをお使いの場合、バックアップファイルを紛失したり、パスワードを忘れたりすると、セキュリティチップが利用できなくなります。
また、セキュリティチップでフォルダやファイルの暗号化を行っている場合、バックアップファイルがないと、データが読み出せなくなることがあります。
これによる損害などの責任は一切負いかねますので、あらかじめご了承ください。
バックアップについては、『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧ください。

### □セキュリティチップをお使いの場合

・リストアは、セキュリティチップの所有者パスワードによって保護されています。そのため、リストアはセキュリティチップの「所有者」が行う必要があります。
・手順に従わずにファイルや設定の変更を行うと、セキュリティチップで管理していた環境が利用できなくなることがあります。

## ユーザー情報の管理

SMARTACCESS のユーザー情報を他のコンピュータで使う場合、次の手順で行います。

**1 バックアップツールでバックアップファイルを作成します。**

**2 利用するコンピュータに SMARTACCESS がインストールされた状態で、バックアップファイルの復元を行います。**

詳しくは、『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧ください。

## コンピュータの修理や保守を依頼する場合

### ■修理前に必要な作業

#### □バックアップ

『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧になり、バックアップを行います。

### □「SMARTACCESS による Windows ログオン」を使用しない設定に変更する

必ず「SMARTACCESS による Windows ログオン」の設定を解除してください。
「SMARTACCESS による Windows ログオン」の設定を解除していないと、修理や保守ができないことがあります。
また、「SMARTACCESS による Windows ログオン」の設定を解除せずに、修理すると、Windows にログオンできなくなることがあります。
解除の手順は次のとおりです。

**1 SMARTACCESS をインストールしたときと同じアカウントで Windows にログオンします。**

**1 「環境設定」を起動します（→ P.34）。**

**2 「設定項目一覧」から「ログオン認証」→「Windows ログオン」の順にクリックします。**

**3 パスワードの自動生成を行っている場合は、パスワードの自動生成を「しない」に設定します。**

パスワードの自動生成を行っていない場合は、手順 5 に進んでください。

**4 次の手順で Windows パスワードを任意のパスワードに変更します。**

1.「スタート」ボタン→「コントロールパネル」の順にクリックします。
　「コントロールパネル」ウィンドウが表示されます。
2.「ユーザー アカウント」をクリックします。
- Windows Vista の場合
  1.「ユーザーアカウントの追加または削除」をクリックします。
  2.「ユーザーアカウント制御」ウィンドウが表示された場合は、「続行」をクリックします。
  「ユーザー アカウント」ウィンドウが表示されます。
- Windows XP の場合
  「ユーザー アカウント」ウィンドウが表示されます。

3. パスワードを変更するアカウントをクリックします。
4. 次の操作をします。
- Windows Vista の場合
  「パスワードの変更」をクリックします。
- Windows XP の場合
  「パスワードを変更する」をクリックします。

この後はメッセージに従って操作します。

**5 「SMARTACCESS による Windows ログオン」の「使用しない」にチェックし、「OK」をクリックします。**

詳しくは、『リファレンスガイド』の「機能編」－「ログオン認証」－「Windows ログオン」をご覧ください。

### □BIOS の設定を変更する

コンピュータ本体の『製品ガイド』の「BIOS」－「BIOS のパスワード機能を使う」をご覧になり、設定した管理者用パスワードを解除します。

### スマートカードをお使いの場合

コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧になり、スマートカードによるロックを使用しない設定にします。

## ■修理後に必要な作業

### □リストア

『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧になり、リストアを行います。
リストアは、パスワードの入力などが必要なため、弊社で行うことはできません。

#### □BIOS の設定を変更する

コンピュータ本体の『製品ガイド』の「BIOS」－「BIOS のパスワード機能を使う」をご覧になり、パスワードを設定します。

#### スマートカードをお使いの場合

コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧になり、スマートカードによるロックを使用する設定にします。

#### □「SMARTACCESS による Windows ログオン」を使用する設定に変更する

「SMARTACCESS による Windows ログオン」を使用していた場合は、『リファレンスガイド』の「機能編」－「ログオン認証」－「Windows ログオン」をご覧になり、「SMARTACCESS による Windows ログオン」の設定を「する」に変更してください。
セキュリティチップをお使いで「機器監査」機能をお使いになる場合、「SMARTACCESS による Windows ログオン」の設定を変更する前に、「現在の機器構成情報の登録」を行う必要があります。

## FeliCa 対応リーダ／ライタをお使いの場合の注意事項

コンピュータ本体のリカバリを実行した場合、FeliCa 対応リーダ／ライタのユーティリティを再インストールする必要があります。
FeliCa 対応リーダ／ライタのユーティリティのインストールについては、「認証デバイスのインストール」（→P.19）をご覧ください。

## セキュリティチップをお使いの場合の注意事項

### ■コンピュータをリカバリする場合、または SMARTACCESS を再インストールする場合

認証デバイスとしてセキュリティチップがインストールされている環境でリカバリをする場合、または SMARTACCESS を再インストールする場合は、あらかじめ BIOS セットアップでセキュリティチップのクリアをする必要があります。
セキュリティチップのクリアについては、コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧ください。
なお、セキュリティチップで管理されている鍵や証明書の情報を引き続きお使いになるには、SMARTACCESS をアンインストールしてセキュリティチップをクリアする前にバックアップし、再インストール後にリストアを行なう必要があります。これを行わない場合、それまで使用していた鍵や証明書が使用できなくなります。
バックアップとリストアの手順については、『リファレンスガイド』の「ツール編」－「オプションツール」－「バックアップツール」をご覧ください。

### ■ハードウェアの変更を行う場合

「機器監査」機能をお使いの場合、ハードウェアの設定を変更すると、Windows にログオンできなくなることがあります。ハードウェアの変更を行う前には必ず、「SMARTACCESS による Windows ログオン」を使用しない設定に変更してください。「パスワードの自動生成」を行っている場合は、一度「パスワードの自動生成」の設定を解除した後、「パスワードの変更」より任意のパスワードに変更してから「SMARTACCESS による Windows ログオン」機能の解除を行ってください。
また、ハードウェアの変更後に、再度「現在の機器構成情報の登録」を行う必要があります。
詳しくは『リファレンスガイド』の「機能編」－「ログオン認証」－「Windows ログオン」をご覧ください。

## ■コンピュータを廃棄する場合

コンピュータを廃棄する場合、コンピュータに残ったデータを復元できないようにすることが重要です。セキュリティチップにより保護されたデータは、セキュリティチップのクリアをし、復元用ファイルを破棄することで復元することができなくなります。
次の手順に従って、セキュリティチップのクリアとハードディスク内のデータ削除を行ってください。

**重要**

- セキュリティチップのクリアをすると、セキュリティチップで暗号化したファイルや証明書が利用できなくなります。
  削除する前に、必要に応じて暗号化を解除してください。
- セキュリティチップのクリアをしても、ハードディスク内のデータは破棄されません。
  セキュリティチップで保護されたハードディスク内のデータは見ることができなくなりますが、必ずハードディスクのデータも削除してください。

**1** **セキュリティチップのクリアをします。**

クリアの手順については、コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧ください。

**2** **コンピュータ本体の『製品ガイド』の「セキュリティ」－「パソコン本体廃棄時のセキュリティ」をご覧になり、ハードディスク内のデータを削除します。**

# 2 指紋センサーについてのトラブルシューティング

### □指紋登録時にエラー表示される

・指の置き方が正しいか確認してください。指が正しく置かれていない、または、指を置く方向が毎回ずれていると登録できないことがあります（→ P.88）。
・指が乾燥していませんか。
手を洗う、指に息を吹きかけるなど指がしっとりする程度の湿り気を与えることで改善されることがあります（→ P.90）。
・指が濡れていませんか。
乾いたハンカチなどで指の湿り気を拭き取ることで改善されることがあります（→ P.90）。
・センサー表面を確認してください。汚れていたり、汗などの水分が付着していると指紋が読み取れない場合があります（→ P.90）。
・異なる指で再度登録してください。

### □指紋照合時にエラー表示される

・指の置き方が正しいか確認してください。指が正しく置かれていないと照合できないことがあります（→ P.88）。
・指が乾燥していませんか。
手を洗う、指に息を吹きかけるなど指がしっとりする程度の湿り気を与えることで改善されることがあります（→ P.90）。
・指が濡れていませんか。
乾いたハンカチなどで指の湿り気を拭き取ることで改善されることがあります（→ P.90）。
・センサー表面を確認してください。汚れていたり、汗などの水分が付着していると指紋が読み取れない場合があります（→ P.90）。
・登録したもう片方の指で照合してください。

### □指をスライドさせても指紋が映らない

・指が乾燥していませんか。
手を洗う、指に息を吹きかけるなど指がしっとりする程度湿り気を与えることで改善されることがあります（→ P.90）。
・センサー表面を確認してください。汚れていたり、汗などの水分が付着していると読み取れない場合があります（→ P.90）。

## ■エラーメッセージ一覧

**・手前側が映っていません。**
指を水平にして、指紋の中心が読み取れるようにまっすぐ引いてください（→ P.88）。
**・指の動きが早過ぎます。**
もう少し指をゆっくりスライドさせてください（→ P.89）。
**・指の動きが遅過ぎます。**
もう少し指を速くスライドさせてください（→ P.89）。
**・指の動かし方が適切ではありません。**
指のスライドのさせ方が正しいか確認してください。指紋の中心が読み取れるようにまっすぐ引いてください（→ P.88）。
**・指が止まったままです。**
指をスライドさせてください（→ P.88）。
**・スライドする距離が短いです。**
指をもう少しセンサーに押し付けてセンサーの中央で指紋の中心が読みとれるようにまっすぐ引いてください（→ P.88）。
**・センサーの左側しか触れていません。**
センサーの中央で指紋の中心が読み取れるようにまっすぐ引いてください（→ P.88）。

・センサーの右側しか触れていません。

センサーの中央で指紋の中心が読み取れるようにまっすぐ引いてください（→ P.88）。

・充分な特徴点が得られませんでした。

- 指が濡れていませんか。
  乾いたハンカチなどで指の湿り気を拭き取ることで改善されることがあります（→ P.90）。
- 異なる指で再度登録してください（→ P.42）。

・登録エラー：同じ指紋と判断できません。もう一度登録を行ってください。

- 指のスライドのさせ方が正しいか確認してください。指紋の中心が読み取れるようにまっすぐ引いてください。（→ P.88）。
- 異なる指で再度登録してください（→ P.42）。

・指紋センサーの起動に失敗しました。

ドライバを正しくインストールしていますか。デバイスマネージャに「AuthenTec Inc.AES2501A」または「AuthenTec Inc.AES2501」と表示されていない場合、または表示されているが、その前に「！」が表示されている場合はドライバをもう一度インストールしてください（→ P.19）。

# 3 FeliCa 対応リーダ／ライタについてのトラブルシューティング

### □BIOS セットアップの「FeliCa デバイス」の設定を「使用しない」にしたら、Windows にログオンできなくなった

FeliCa 対応非接触 IC カードを使って Windows ログオンを行っている場合は、BIOS セットアップの「FeliCa デバイス」の設定を「使用する」にしてください。BIOS セットアップの設定については、コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧ください。

### □FeliCa のドライバ（Sony FeliCa リーダー / ライターソフトウェア）をアンインストールすると、Windows が起動できなくなる

FeliCaのドライバをアンインストールするときは、SMARTACCESSをアンインストールした後で行ってください。
FeliCaのドライバのアンインストールについては、「認証デバイスのアンインストール」（→P.29）をご覧ください。
FeliCaのドライバがインストールされていない状態でSMARTACCESSによるログオンを行うとWindowsが正常に起動できなくなります。Windowsが正常に起動できなくなった場合はご購入元にお問い合わせいただくか、コンピュータ本体の『取扱説明書』をご覧になり、弊社までお問い合わせください。

# 4 スマートカードリーダ／ライタ、スマートカードホルダーについてのトラブルシューティング

スマートカードリーダ／ライタ、およびスマートカードホルダーをお使いのときに表示されるエラーメッセージについては、コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧ください。

# 5 セキュリティチップについてのトラブルシューティング

### □BIOS でセキュリティチップの設定を変更できない

BIOS で、セキュリティチップの使用や、セキュリティチップのデータをクリアする設定を行うためには、管理者用パスワードの設定が必要です。管理者用パスワードが設定されているか確認してください。

### □Infineon TPM Professional Package（Infineon Security Platform）ユーティリティがインストールできない

ソフトウェアをインストールするには、BIOS でセキュリティチップを使用する設定になっている必要があります。BIOS の設定を確認してください。
BIOS の設定については、コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧ください。

### □Windows ログオン時に機器構成が変更された旨のエラーメッセージが表示される

前回の起動時からハードウェアの構成や設定が変更された可能性があり、SMARTACCESS の機器監査機能によりメッセージが表示されています。ハードウェア構成や BIOS 設定などが変更されていないか確認してください。
変更があった場合は、機器を登録したときの状態に戻すか、ハードウェアの構成を登録し直してください。
なお、変更の内容によっては、機器を登録したときの状態に戻しても、エラーメッセージが解除されない場合があります。詳しくは『リファレンスガイド』の「機能編」－「ログオン認証」－「機器監査」をご覧ください。

### □Windows ログオン時に機器構成が変更された旨のメッセージが表示され、Windows にログオンできなくなった

前回の起動時から、ハードウェアの構成や設定が変更された可能性があり、SMARTACCESS の機器監査機能により Windows にログオンできなくなっています。
ハードウェア構成や BIOS 設定などが変更されていないか確認してください。
変更があった場合はハードウェアの構成を登録したときの設定に戻すか、ハードウェアの構成を登録し直してください。
詳しくは『リファレンスガイド』の「機能編」－「ログオン認証」－「機器監査」をご覧ください。

### □Windows ログオン時にユーザーキーパスワードエラーになる

SMARTACCESS による Windows ログオンを有効にしている場合には、Windows のパスワードではなくセキュリティチップのユーザーキーパスワードを入力してください。

### □EFS が利用できない

EFS を利用するにはハードディスクが NTFS でフォーマットされていることが必要です。FAT32 のドライブでは EFS を利用することはできません。なお、Windows XP Home Edition では、EFS は利用できません。

### □BIOSセットアップでセキュリティチップを変更したら、Windowsにログオンできなくなった

セキュリティチップをお使いになる場合、BIOS セットアップのセキュリティチップの設定は次のようになっている必要があります。

・FMV-ESPRIMO、FMV ロングライフパソコン、CELSIUS シリーズの場合
  - Security Chip: **「Enabled」**
  - Security Chip State: **「Enabled and Activated」**（表示がある場合）

・FMV-LIFEBOOK、FMVSTYLISTIC の場合
  - セキュリティチップ : **「使用する」**
  - セキュリティチップの状態 : **「有効かつ使用可」**（表示がある場合）

「SMARTACCESS による Windows ログオン」を「する」に設定した状態で、BIOS セットアップのセキュリティチップの設定を変更すると、セキュリティチップに保存していた Windows パスワードが利用できず、Windows にログオンできなくなることがあります。その場合は BIOS の設定を上記のように設定し直すか、「回避パスワード」でログオンする必要があります。
BIOS の設定については、コンピュータ本体の『製品ガイド』の「BIOS」－「認証デバイスのセキュリティ機能を使う」をご覧ください。
なお、「回避パスワード」でログオンしても、セキュリティチップで保護された環境は安全に管理されています。
回避パスワードについては、『リファレンスガイド』の「機能編」－「ログオン認証」－「Windows ログオン」－「認証回避」をご覧ください。

### □リストアを行うとユーザーキーパスワードが変わることがある

リストアを行うと、ユーザーキーパスワードにはバックアップを行った時点でのパスワードが設定されます。
そのため、バックアップ後にユーザーキーパスワードを変更しても、復元すると、バックアップを行った時点でのパスワードに戻ります。

### □ソフトウェアのインストール時に「アプリケーションエラー」が表示されることがある

「インストール」（→ P.17）の手順に従わずにソフトウェアをインストールすると、「アプリケーションエラー」が表示されることがあります。
もし表示された場合、ソフトウェアのインストールを引き続き行い、インストール終了後は表示画面に従って Windows を再起動してください。再起動後は正常に動作します。

### □SMARTACCESS でユーザー初期化を行うと、失敗することがある

SMARTACCESS をインストール時に、セキュリティチップがクリアされていない状態で行うと、ユーザー初期化に失敗することがあります。インストール時にはセキュリティチップがクリアされていたかどうか確認してください。クリアされていなかった場合には SMARTACCESS をアンインストールし、BIOS でセキュリティチップをクリアした後、再度 SMARTACCESS をインストールしてください。

### □インストール時に「所有者のパスワードの設定に失敗しました。Infineon TPM Professional Package がインストールされていません。」と表示される

・BIOS セットアップで、「セキュリティチップを使用する」または「有効」に設定されていることを確認してください。「セキュリティチップを使用する」または「有効」に設定されてされていない場合は、SMARTACCESS をアンインストールし、「セキュリティチップを使用する」または「有効」に設定後、再度 SMARTACCESS をインストールしてください。
・Infineon TPM Professional Package がインストールしてあることを確認してください。Infineon TPM Professional Package がインストールしてある場合は、SMARTACCESS をアンインストールし、Infineon TPM Professional Package をアンインストール後、再度 Infineon TPM Professional Package をインストールし、SMARTACCESS をインストールし直してください。

# 6 その他のトラブルシューティング

## 認証デバイスなしで Windows にログオンしたい

認証デバイスを忘れたり、紛失したり、破損したりしたとき、または、認証デバイスの所有者が不在のときに Windows にログオンする必要がある場合、Windows 標準のログオンウィンドウから認証デバイスを使わずにログオンすることができます。
詳しくは『リファレンスガイド』の「付録」－「トラブルシューティング」－「Windows ログオンに関するトラブルシューティング」をご覧ください。

## その他

このマニュアルに記載されていないトラブルやエラーメッセージの対処方法については、『リファレンスガイド』の「付録」－「トラブルシューティング」をご覧ください。

### ■お問い合わせ先

技術的なご相談については、ご購入元にお問い合わせいただくか、『リファレンスガイド』の「付録」－「トラブルシューティング」－「お問い合わせ先」をご覧になり弊社までお問い合わせください。

第 7 章

# 付録

# 用語集

| 用語 | 説明 |
|---|---|
| Active Directory | Windows Server のディレクトリ サービスで、Windows Server の分散ネットワークの基盤となるものです。 |
| PIN（Personal Identification Number） | IC カード（FeliCa 方式）やスマートカードを使うときのパスワードの一種です。 |
| Portshutter | コンピュータの各種ポートを使用制限できるソフトウェアです。FMV シリーズや CELSIUS シリーズのコンピュータに添付されています。 |
| Security Platform（Infineon TPM Professional Package） | セキュリティチップを使用するために必要なユーティリティです。 |
| SMARTACCESS アカウント | SMARTACCESS を利用するためのアカウント情報です。ユーザー名とパスワードを登録します。 |
| Windows ログオン情報 | 認証デバイスに登録する、Windowsにログオンするときのユーザー名、パスワード、ドメイン名などです。 |
| アプリケーションログオン情報 | 認証デバイスに登録するソフトウェアやWebサイトにログオンするときのユーザー名、パスワードなどです。 |
| 暗号鍵 | 情報を暗号化または復号するときに使用する、特定のデータです。 |
| カード IDm | IC カード（FeliCa 方式）のシリアル番号です。カード製造時に一意に割り当てられます（カードに刻印された番号とは異なります）。 |
| カード抜き取り | IC カード（FeliCa 方式）やスマートカードをセットした状態から外す操作です。 |
| カードのポーリング動作 | スマートカードをリーダ／ライタから抜き取ったり、IC カード（FeliCa 方式）をリーダ／ライタにタッチしたりしたときに、コンピュータのロックや強制ログオフなどを行い、コンピュータを不正な使用から保護することです。 |
| 管理者 | SMARTACCESS で設定したセキュリティ環境を管理する人（セキュリティポリシーを設定したり、管理したりする人）です。<br>通常、Windows アカウントは管理者（Administrators）権限です。 |
| 管理者 PIN | 管理機能を利用する場合に必要となる PIN です。 |
| 管理者権限カード | カード管理リストで、管理者属性が設定されているカードです。 |
| 機器監査 | あらかじめ機器構成を登録し、Windows 起動時の機器構成と比較することで、機器構成が変更されていないかを監査する機能です。 |
| 機器構成 | BIOS 設定のハードウェア構成やメモリスロットの構成など、使用しているコンピュータのハードウェア構成です。 |
| 証明書 | 本人を証明する電子証明書のことです。SMARTACCESSでは、Windows ログオンやWebサーバーへのアクセスにお使いになれます。 |
| 所有者 | IC カード（FeliCa 方式）やスマートカードなど、持ち運び可能な認証デバイスを所有する人です。 |
| 所有者 PIN | 通常使用する PIN です。 |
| シングルサインオン機能 | ソフトウェアや Web サイトなどにログオンするとき、一度ログオン認証に成功すれば、以降は同一ユーザーがコンピュータを継続使用しているものとしてログオン認証を省略できるようになる機能です。 |
| セキュリティチップ | TPM（Trusted Platform Module）と呼ばれるセキュリティ用の専用ハードウェアチップです。<br>セキュリティチップは内部に暗号鍵を保持し、ソフトウェアで使用するパスワードなどを暗号化します。セキュリティチップに保持された暗号鍵は外部に出す方法がありませんので安全に管理できます。 |
| セット | IC カード（FeliCa 方式）を FeliCa 対応リーダ／ライタに載せておくことです。 |
| タッチ | IC カード（FeliCa 方式）を FeliCa 対応リーダ／ライタに一時的に接触させる操作です。 |

| 用語 | 説明 |
| --- | --- |
| 認証デバイス | 認証を行う手段や装置です。<br>SMARTACCESS では、セキュリティチップ、指紋センサー、FeliCa 対応リーダ／ライタ、スマートカードリーダ／ライタ、およびスマートカードホルダーを指します。 |
| バイオパスワード | 指紋を登録するときや、指紋でのログオンを回避するときに使用するパスワードです。 |
| ユーザーキーパスワード | セキュリティチップを使用する際に入力するパスワードです。セキュリティチップを使用するユーザー毎に設定します。基本ユーザーパスワードと表現されることもあります。 |
| ユーザー情報 | Windowsログオン情報およびアプリケーションログオン情報などの認証用の情報のことです。例えば、ユーザー名やパスワード、指紋、PIN などを指します。 |
| 利用者 | SMARTACCESS で設定したセキュリティ環境を管理者のもとで使う人です。 |
| 連携ソフトウェア | SMARTACCESS の機能を拡張させるために、連携できる他製品の総称です。このマニュアルでは Portshutter です。 |